The Politics of Cyberspace in Iran: State-society and International Relations in the Information Age

by

Roozbeh Safshekan Esfahani

A thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Political Science
University of Alberta

ABSTRACT

Cyberspace is a domain accommodating an unprecedented level of human activity and social relations, with significant implications for domestic politics and international relations. Despite the growing significance of cyberspace in politics, it has received relatively little attention in the scholarly literature, especially with regard to the measures that states are adopting to manage this emerging domain of power. The Islamic Republic of Iran (IRI) provides a strong case study for understanding this dynamic, having experienced the full spectrum of opportunities and risks associated with the exercise of power in cyberspace. Using the IRI as a case study, this dissertation asks: *what measures has the IRI adopted to manage the risks and opportunities of cyberspace as an emerging domain of power, and how have these measures interacted with Iranian state-society and international relations?*

This dissertation criticizes the materialist and state-centric concept of power in structural realism as an inadequate analytical tool for examining how power is exercised in cyberspace. In order to suggest an inclusive conceptualization of power, which highlights the significance of ideational factors and non-state actors in the exercise of power in cyberspace, this dissertation draws on the theoretical frameworks of Robert W. Cox and Joseph S. Nye, distinguishing between four major types of power: coercive power; economic power; power embedded in international institutions; and co-optive power generated from ideational sources. The exercise of each type of power in Iranian cyberspace is examined in a separate chapter by using a hybrid methodology suitable for analyzing quantitative and qualitative data collected from online public documents, academic

literature on cyberpolitics, semi-structured interviews, raw technical and macro-economic data, and social media data.

First, this dissertation identifies the main pillars through which the IRI exercises coercive power in cyberspace at the domestic level, showing how they limit Iranian users' access to information and compromise their online security. These pillars are the national information network; comprehensive regime of filtering; and restrictive body of law regulating cyber activities and the law enforcement organizations that implement it. The dissertation also examines the IRI's exercise of coercive power at the global level and identifies the main defensive and offensive cyber measures taken by the IRI to establish deterrence against foreign adversaries.

Second, the dissertation examines the measures adopted by the IRI to exploit the significant potential of cyberspace for economic development. Using four main global indexes of information and communication technology development, this study compares the impact of cyberspace on the Iranian economy against the impact on a sample of economies in the Caucasus, Central Asia, and Middle East regions. The analysis of these indexes illustrates the IRI has fallen short of meeting the ambitious goals that it has set for itself in its core development documents.

Third, the dissertation studies the policies promoted by the IRI to govern cyberspace through international institutions of Internet governance. Analyzing the official documents of six major global forums on Internet governance, the research finds that the IRI agenda is mainly preoccupied with the issues of the digital divide and what it perceives as the negative role of Global North countries and non-state actors in Internet Governance. The analysis shows that

overemphasis on these issues led the IRI to ignore the complexity of the emerging regime of global Internet Governance and, consequently, to overlook pervasive issues such as transnational cybercrime.

Fourth, this dissertation examines how effectively moderates and principlists, the IRI's two main political currents, utilize cyberspace to generate the ideational sources of co-optive power. Analyzing the online content generated by the selected moderate and principlist figures and the level of content generation and user engagement they spawn, the research finds that moderates exert strong influence over the generation of ideational sources in Iranian cyberspace. The analysis also finds that principlists have recently made the shift from a reactive to proactive approach to cyberspace and actively engaged in an online competition with moderates over the generation of ideational sources. When it comes to user engagement, however, principlists still lag behind moderates.

PREFACE

This thesis is an original work by Roozbeh Safshekan Esfahani. A version of chapter five of this thesis has been published as: Safshekan, Roozbeh. "Iran and the Global Politics of Internet Governance." *Journal of Cyber Policy* 2.2 (2017): 266-84.

ACKNOWLEDGMENTS

Many individuals helped me during my doctoral studies at the University of Alberta to whom I am deeply indebted. First and foremost, I would like to thank my supervisor, Mojtaba Mahdavi, for his knowledge and expertise, without which the completion of this dissertation would have been hardly possible. Throughout my doctoral research, I learned a great deal from him and benefitted tremendously from his guidance and assistance, while always enjoying the liberty he kindly gave me to determine the direction of my research and draw my own conclusions.

I owe a great deal to the other members of my supervisory committee, Roger Epp and Thomas Keating, whose invaluable comments and suggestions enormously helped me to refine various aspects of my research agenda and improve the quality of my dissertation. I am also thankful to Zohreh Bayatrizi and Ashley Esarey for their insightful feedback on my doctoral proposal and the earlier drafts of this dissertation.

I am very grateful to the Social Sciences and Humanities Research Council of Canada (SSHRC) for recognizing the value of my doctoral research and awarding me a three-year Joseph-Armand Bombardier CGS Doctoral Scholarship. I would also like to thank the interviewees who accepted to participate in this research and generously shared their time with me to answer my questions.

I owe a great debt to my parents for their unconditional love and support throughout my whole life and I can not thank them enough for the encouragement and motivation they gave me during my doctoral studies. I will be forever indebted to my loving wife and best friend, Mina Gheiratmand, for giving me all of her kindness and support. It is to her that I dedicate this dissertation.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Cyberspace is an emerging domain of power where both state and non-state actors engage each other on a regular basis, impacting state-society and international relations.[1] Nearly all governments, to a greater or lesser extent, have engaged in cyber monitoring of their citizens. One of the most egregious examples of mass surveillance by a state over its citizens has been the program carried out by the National Security Agency (NSA) as revealed by Edward Snowden.[2] Another is the revelation of the British Government Communication Headquarters' (GCHQ) targeting of critics, journalists, and researchers who shed light on government activities.[3] Cyber censorship, in which governments filter Internet content, is regularly practiced in China, whose "Great Firewall" is one of the most pervasive systems of censorship,[4] and Turkey which famously blocked Twitter during the Gezi Park demonstrations.[5] The United States, with all its mighty intelligence and counterintelligence capabilities, has been the target of systematic cyber industrial espionage for many years not only by its rival China, but most likely by its closest ally Israel as well.[6] Russia, for its part, was among the first states to conduct offensive operations in

---

[1] Choucri, Nazli, and Daniel Goldsmith. "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security." *Bulletin of the Atomic Scientists* 68.2 (2012): 70-77.

[2] Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. New York, NY: Metropolitan Books, 2014.

[3] Ball, James. "GCHQ Captured Emails of Journalists from Top International Media." *The Guardian.* 19 Jan. 2015. Web. 07 Apr. 2018. <https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post>.

[4] Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT, 2010. p.4.

[5] Ozbilgin, Ozge. *Turkey Tightens Internet Controls, Weeks into New Government*. Sept. 2014. Web. 02 Jan. 2015. <https://www.reuters.com/article/us-turkey-internet/turkey-tightens-internet-controls-weeks-into-new-government-idUSKBN0H419T20140909>.

[6] Stein, Jeff. "The Latest Document From the Snowden Trove Highlights Israeli Spying." *Newsweek*.16 May 2014. Web. 07 Apr. 2018. <http://www.newsweek.com/mostly-good-week-israel-us-spying-controversy-251261>.

cyberspace at a time of war during its conflict with Georgia.[7] Social movements challenging government authority in different countries all across the globe, from the Tibet Movement[8] to the Arab Spring to Occupy Wall Street,[9] utilize cyberspace as a key element of their communication strategy. As these examples demonstrate, cyberspace presents state and non-state actors with opportunities for gaining power and risks for losing it. Given the challenges cyberspace poses to territorial forms of rule, states in particular are confronted with the need to manage this emerging domain of power. Despite the growing significance of cyberspace as a domain of power, it has received relatively scant attention in the scholarly literature. This is especially true in terms of case-studies that comprehensively analyze measures that states are adopting domestically and globally to manage the opportunities and risks associated with cyberspace. These relatively new measures are likely to shape and reshape both state-society and international relations of states in the years to come.

Research Topic

The Islamic Republic of Iran (IRI) is a strong case study for understanding the emerging dynamics illustrated above. It has experienced the full spectrum of opportunities and risks associated with the exercise of power in cyberspace. The Stuxnet worm in 2010, which targeted industrial systems underlying the Iranian nuclear program, and specifically its uranium enrichment infrastructure, is a prime example of a cyber risk posed by state rivals at the

---

[7] Deibert, Ronald, et al. “Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War.” *Security Dialogue* 43.1 (2012): 3–24.

[8] Tibet Action Institute. "Tibet: Frontline of the New Cyberwar." *YouTube*, 27 Jan. 2015. Web. 07 Apr. 2018. <http://www.youtube.com/watch?v=yE3AQqbGVkk.%2BAccessed%2B1%2BFeb.%2B2015.>.

[9] Gerbaudo, Paolo. *Tweets and the Streets: Social Media and Contemporary Activism*. London: Pluto Press, 2012.

international level.[10] The 2009 Green Movement, which utilized cyberspace as the crux of its communication strategy and threatened the political stability of the state, is another example of a cyber risk but at the domestic-level.[11] The salience of this experience was most recently confirmed by the Iran protests of December 2017 and January 2018, which saw demonstrators utilize the widely popular Telegram messaging application to communicate and organize. The protests, which included thousands of people across more than 70 cities,[12] were perceived as such a challenge by Iranian authorities that they felt compelled to temporarily filter Telegram.

On the other hand, the IRI has found opportunities in cyberspace. For example, it used cyber-warfare to attack the Saudi Arabian national oil company's IT systems, generating considerable costs for the Saudis, without paying as high a price as it would otherwise have had these attacks been carried out in another domain of power such as land, sea, air, or space.[13] Likewise, cyberspace has provided the IRI with greater opportunities for surveilling Iranian society, giving it access to a higher quality and quantity of personal information than was ever possible in the past. In order to manage these opportunities and risks, the IRI has formulated a broad range of measures which manifest themselves in a number of institutions and projects, including the National Information Network (NIN), comprehensive regime of Internet filtering, cyber police, and cyber army.

---

[10] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown Publishers, 2014; Collins, Sean, and Stephen Mccombie. "Stuxnet: the Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7.1 (2012): 80–91.

[11] Yahyanejad, Mehdi. "The Effectiveness of Internet for Informing and Mobilizing in the Events after the Iranian Presidential Election." *Massachusetts Institute of Technology (MIT)*. 2010. Web. 07 Apr. 2018. <groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2010/weeks/week12-Yahyenejad.pdf>.

[12] Asadzade, Peyman. "New Data Shed Light on the Dramatic Protests in Iran." *The Washington Post*. 12 Jan. 2018. Web. 05 May 2018. <https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/12/what-data-show-us-about-irans-protests/?utm_term>.

[13] Bronk, Christopher, and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco." *Survival* 55.2 (2013): 81–96.

The existing academic literature has mainly focused on how Iranian society uses cyberspace to advance its varied goals.[14] Yet a comprehensive case study examining the measures taken by the IRI to manage cyberspace does not exist. The objective of the present doctoral project is to fill this gap in the literature. Using the IRI as a case study, this project asks: *what measures has the IRI adopted to manage the risks and opportunities of cyberspace as an emerging domain of power, and how have these measures interacted with Iranian state-society and international relations?*

As will be shown in the literature review, some elements of the measures taken by the IRI - such as the comprehensive regime of filtering - have been previously studied to some degree. The yet to be explored elements researched in this dissertation include: the National Information Network (NIN); the restrictive body of law and the organizations that enforce it; defensive and offensive measures the IRI takes to establish deterrence against its adversaries at the global level; the state of the Iranian cyber economy and ICT development; the IRI's global Internet governance agenda;[15] and, lastly, the efforts by government officials and public figures to utilize cyberspace to propagate their favored political and social agenda by generating and debating different ideational factors associated with political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. The present research project seeks to contribute to the academic literature on the politics of cyberspace in

---

[14] Sreberny, Annabelle, and Gholam Khiabany. Blogistan: *The Internet and Politics in Iran*. London: I.B. Tauris, 2010; Faris, David M., and Babak Rahimi, eds. *Social Media in Iran: Politics and Society after 2009*. Albany: NY: State University of New York, 2015; Akhavan, Niki. *Electronic Iran: The Cultural Politics of an Online Evolution*. New Brunswick: Rutgers University Press, 2013; Kelly, John, and Bruce Etling. "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere." *The Berkman Klein Center for Internet & Society at Harvard University*. April 2008. Web. 07 Apr. 2018. <https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf>.

[15] The chapter on this element has already appeared as a journal article in the Journal of Cyber Policy by Chatham House. See: Safshekan, Roozbeh. "Iran and the Global Politics of Internet Governance." *Journal of Cyber Policy* 2.2 (2017): 266-84.

Iran by deepening the level of insight on the previously investigated elements, and establishing a baseline for the elements that have yet to be examined, all within a coherent theoretical framework.

Research Background: The Contested Political Implications of Cyberspace

How does the exercise of power in cyberspace impact the state-society and international relations? The answers to these questions are contested in the academic literature. At the level of domestic politics, some scholars argue that because cyberspace does not favor centralized hierarchical forms of organization, it can be empowering for the individual and shift the balance of power in favor of society over the state. Following leading scholars such as Ithiel de Sola Pool, the figures of this genre generally characterize cyber technologies as "technologies of freedom".[16] The scholars who emphasize the liberating and democratizing potential of cyberspace can be divided into three main groups. The first group foresees the realization of the age-old dream of direct democracy through cyberspace, with individual citizens being able to exercise their political preferences through online elections, referenda and opinion polls.[17] The second group touts the community-building aspects of cyberspace, not only for geographically-defined communities but also for a potentially infinite number of virtual communities which can facilitate collective action on specific issues and causes.[18] The third group, following Habermas' concept of the "public sphere" where people can engage in critical debate on issues of mutual concern, sees cyberspace as new fora for public debate which is more inclusive than what has

---

[16] Pool, Ithiel de Sola. *Technologies of Freedom*. Cambridge, MA: Harvard University Press, 1983.

[17] Adonis, Andrew, and Geoff Mulgan. "Back to Greece: The Scope for Direct Democracy." *Demos Quarterly* 3 (1994): 1-28.

[18] Etzioni, Amitai. "Are Virtual and Democratic Communities Feasible?" *Democracy and New Media*. Ed. Henry Jenkins and David Thorburn. Cambridge, MA: MIT Press, 2004. 85–100.

existed prior.[19] Recalling Habermas' view of the historical impact of the printing press, which he saw as facilitating the democratization of Europe by providing room for debate and consensus-building by a politically active citizenry,[20] this group of scholars sees strong parallels between the political implications of the nineteenth century printing press and that of cyberspace today. In contrast, other scholars believe that the state will eventually be able to overcome the democratic potential and power diffusing nature of cyberspace, and use it to enhance state power and heighten repression. David Noble, a technology historian, has warned that: "Visions of democratization and popular empowerment via the net are dangerous delusions; whatever the gains, they are overwhelmingly overshadowed and more than nullified by the losses".[21] Evgeny Morozov asserts that these losses can range "from the sprawling surveillance apparatus facilitated by the public nature of social networking to the persistence of myth making and propaganda, which is much easier to produce and distribute in a world where every fringe movement blogs, tweets, and Facebooks".[22]

Another line of argument affirming the emancipatory power of cyberspace is that the Internet has enabled greater transparency and interactivity on the part of the state. Premised on a Weberian view of bureaucratic organizations as a "machine", this group of scholars emphasizes the role of

---

[19] Becker, Barbara, and Josef Wehner. "Electronic Networks and Civil Society: Reflections on Structural Changes in the Public Sphere." *Culture, Technology, Communication: Towards an Intercultural Global Village*. Ed. Charles Ess and Fay Sudweeks. Albany, NY: SUNY Press, 2001. 65-85; Ess, Charles M. "The Political Computer: Democracy, CMC, and Habermas." *Philosophical Perspectives on Computer-Mediated Communication*. Ed. Charles M. Ess. Albany, NY: SUNY Press, 1996. 197–230.

[20] Habermas, Jürgen. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Trans. Thomas Burger. Cambridge, MA: MIT, 1989.

[21] Noble, David. "Computers Will Create Unemployment." *Computers and Society*. Ed. Paul A. Winters. San Diego, CA: Greenhaven, 1997. 40-43.

[22] Morozov, Evgeny. *The Net Delusion the Dark Side of Internet Freedom*. New York, NY: PublicAffairs, 2011. p. 312.

technology in making government's bureaucratic machine more rational and efficient. Helen Margetts, following this approach, sees the proliferation of the Internet and related technologies as allowing for smaller and more efficient government which will eventually wither into irrelevance.[23] In contrast, some scholars see the transformative effects of the Internet on government as being largely negative, with "e-government" being both more powerful and intrusive than traditional governments could have ever hoped to be. More than a decade before the Internet became a fact of daily life, a pioneering figure of this genre David Burnham saw the increased powers of surveillance and control enabled by computer technologies as leading to the "The Rise of the Computer State", which would see the realization of the nightmarish scenario of centralized state control envisioned by George Orwell's 1984.[24]

The academic debates over the impact of cyberspace on state-society relations are also mirrored in international relations. One group of scholars, following figures such as Manuel Castells, argues that the information and communication technology revolution facilitates the globalization process by deepening economic interdependence between states and societies.[25] According to these scholars, interdependent and networked economies of the cyber era will generate not only mutual benefit but mutual interest, creating a dependence between states and peoples that would increase understanding and cooperation while decreasing the use of military power and ultimately "sketches a future with an ever-widening zone of international peace".[26] Another element which can encourage mutual understanding and cooperation among states is

---

[23] Margetts, Helen. *Information Technology in Government: Britain and America*. London: Routledge, 1999.

[24] Burnham, David. *The Rise of the Computer State*. New York, NY: Random House, 1983.

[25] Castells, Manuel. *Information Technology, Globalization and Social Development*. Geneva: UNRISD, 1999.

[26] Rosecrance, Richard N. *The Rise of the Virtual State: Wealth and Power in the Coming Century*. New York, NY: Basic, 1999. p.24.

known as “vulnerability interdependence”. In Cyber War, Richard Clarke and Robert Knake argue that managing the challenges of the current cyber era (e.g: identity theft, data and intellectual property theft, systems crash and interruption of information, cyber terrorism), is not an undertaking that any one state is capable of handling alone, but requires “cooperative strategies” advanced by the global community as a whole.[27] Moreover, cyberspace can encourage the creation of a “global civil society”, including civil society organizations operating across international boundaries and independent from state interests and leadership.[28][29] Empowered by cyberspace to network and grow, such organizations could create the foundation for a novel global public sphere that could change politics by promoting peace over lethal conflicts among the states.

Other scholars, diverging from this line of thought, highlight the potential for cyber warfare and cyber espionage to generate conflict between states. For example, Salma Shaheen argues that offense is favored in cyberspace and the shift of offense-defense balance towards offense in this domain of power makes conflict, rather than cooperation, more likely.[30] In the same vein, Clark and Levin[31] and Lynn III[32] argue that the advantage of offense is compounded by the anonymity afforded by cyberspace, which makes attributing cyber attacks with a high level of confidence difficult or impossible. When added to the low cost of cyber attacks and the relatively higher cost of cyber defense, this means that defense provides little protection against attacks because it

---

[27] Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York, NY: Harper Collins, 2010.

[28] Lipschutz, Ronnie D. "Reconstructing World Politics: The Emergence of Global Civil Society."*Millennium: Journal of International Studies* 21.3 (1992): 389-420.

[29] Castells, Manuel. *The Rise of the Network Society*. Oxford: Blackwell, 1996.

[30] Shaheen, Salma. "Offense–Defense Balance in Cyber Warfare." *Cyberspace and International Relations Theory, Prospects and Challenges*. Ed. Jan-Frederik Kremer and Benedikt Müller. Berlin: Springer Berlin, 2016. 77-94.

[31] Clark, Wesley K., and Peter L. Levin. "Securing the Information Highway." *Foreign Affairs* 88.6 (2009): 2-9.

[32] Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89.5 (2010): 97-108.

imposes little to no cost on an attacker who is free to strike again. This allows states to indulge in an arms race to gain superiority over foes because of the benefits linked with offense. According to Ronald Deibert , there is already “an undeniable arms race occurring in cyberspace, and the domain is being rapidly militarized. Governments around the world now see cyber security as an urgent priority. They are standing shoulder-to-shoulder with their armed forces on this issue, and the capacity to fight and win wars in cyberspace is now seen as an absolute necessity by authoritarian regimes and liberal democracies alike”.[33]

As these debates illustrate, there is no academic consensus on how the exercise of power in cyberspace impacts the state-society and international relations. Keeping in mind this background on the state-of-the-art of the literature, which will be discussed at length in chapter one, case studies can be viewed as essential tools to study this subject matter. Indeed the implications of cyberspace for state-society and international relations can differ depending on the case. Context can be just as important as the characteristics of cyberspace itself in determining what outcomes will play out in the case of a particular state. The case study as a research tool enables us to gain an in-depth understanding of a particular phenomenon. While some observations will be generalizable to cyberspace as a whole, others will be unique to the specific case in question. Comprehensive case studies on the implications of cyberspace for the domestic politics and foreign policy of specific states do exist, particularly for major powers like China. However, at present there is a dearth of comprehensive case studies on many states including the Islamic Republic of Iran. It is therefore the intention of this study to fill this gap in the literature.

---

[33] Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013. p.168.

Chapter Breakdown

This dissertation is divided into six chapters. Chapter one will comprehensively review the academic literature on the implications of cyberspace as an emerging domain of power for state-society and international relations. The chapter will cluster and examine these implications around eight themes. These clustered themes represent eight major debates found by the author in the academic literature on cyberspace relevant to this case study, and include: 1) social mobilization 2) collective action repertoires 3) generating and framing media coverage 4) state propaganda, surveillance, and denial of access 5) international security 6) global economy 7) global cyber governance and 8) public diplomacy. The chapter will illustrate that the political implications of cyberspace can differ, depending on the specific case, with context being just as important as the main characteristics of cyberspace itself in determining what outcomes will play out in a particular state. The chapter will thus highlight the gap in the literature that this dissertation addresses and the potential contributions of this research, specifically completing a comprehensive case study on the IRI's cyber measures and their interaction with Iranian state-society and international relations.

Chapter two provides the theoretical framework of the dissertation. It critiques the materialist and state-centric concept of power, as formulated in structural realism, arguing that it is not an adequate analytical tool for examining how power is exercised in cyberspace. The chapter shows that in order to understand this dynamic, we instead need a synthetic concept of power which also highlights the significance of ideational factors and non-state actors in politics. In order to formulate a more comprehensive and nuanced conceptualization of power that may be

particularly useful for the purpose of this case study, this dissertation draws on the works of Robert W. Cox and Joseph S. Nye, distinguishing between four major types of power: coercive power; economic power; power embedded in international institutions; and co-optive power generated from ideational sources. Their conceptualizations of power acknowledge the role of non-state actors and ideational factors in politics and allow us to not only account for the implications of cyberspace for international relations, but also for state-society relations. The chapter also introduces the research design, rationale behind the single case study method used in this dissertation, and a set of methods for collecting quantitative and qualitative data, including: online public documents, the academic literature on cyberpolitics, semi-structured interviews, raw technical and macro-economic data, and social media data.

Chapter three will examine the four main pillars through which the IRI exercises coercive power in cyberspace in four sections, respectively. Section one looks at the National Information Network project, which has the potential to territorialize Iranian cyberspace and wall it off from the global Internet, thereby limiting Iranian users access to information and compromising their online security. Section two explores the comprehensive regime of filtering as a pillar of coercive power in the context of the IRI's general approach to limiting Iranian society's access to information. Section three studies the Iranian body of law regulating cyber activities and the main law enforcement organizations created for its implementation, aimed at deterring Iranian citizens from cyber activities the IRI deems undesirable. Section four analyses the IRI's defensive measures in the context of the cyber attacks conducted against it by rival state actors. It also elaborates on the offensive measures adopted by the IRI to demonstrate its capability to retaliate against its rivals and establish deterrence.

Chapter four will conduct a study of ICT development in the IRI and compare it against the countries listed in Iran's 2025 Vision Document as peer competitors. This document, one of the corner-stone development documents of the IRI, calls on Iran to become ranked first in terms of economy, science, and technology among the countries of the Caucasus, Central Asia, and Middle East regions by the year 2025. The four indexes that will be utilized in this chapter shed light on different aspects of ICT development, highlighting the strengths and weaknesses of the IRI in exploiting the economic potential of cyberspace. These indexes include: 1) The Economist Intelligence Unit and IBM Institute for Business Value's E-readiness Index (ERI); 2) The United Nations' E-government Development Index (EGDI); 3) The World Economic Forum's Networked Readiness Index (NRI); and 4) The International Telecommunication Union's ICT Development Index (IDI). Thus far, the IRI has fallen short of meeting these ambitious goals that it has set for itself in the 2025 document. The analysis of these indexes will help shed light on the main obstacles in the path of the IRI to achieving these goals.

Chapter five will analyze the Internet Governance agenda pursued by the IRI at international institutions. Surveying the official documents of six major global events on Internet Governance since 2003, this chapter illustrates that the IRI Internet Governance agenda has been shaped and transformed by the interplay of state-society relations and international relations, and preoccupied with three major issues: the digital divide and significant potential of the Internet for economic development; the dominant role of Global North countries in the management of critical Internet resources; and the role of non-state actors in Internet Governance. The latter issue constitutes the main area of contention between different presidential administrations in Iran, which historically have had strong influence over the IRI's Internet governance agenda and

in some instances have diverged from one another on key issues surrounding it. The chapter will also highlight how overemphasis on these three issues by the IRI has led it to ignore the complexity of the emerging regime of global Internet Governance and to overlook important issues, such as transnational cybercrime.

Chapter six will analyze co-optive power relations in Iranian cyberspace, generated from ideational sources such as political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. The chapter will identify top Iranian public figures and government officials who generate these ideational factors in Iranian cyberspace from among the moderates and principlists (also known as conservatives), the two main political currents in the IRI. Quantitative analysis of these two groupings conducted in this chapter based on data collected leading up to the 2017 Iranian presidential election shows that, although moderates often featured more frequently and prominently in the media, principlists were actually also very active in online content generation. When compared to moderates, however, principlists were weaker on user engagement. The qualitative analysis of the online content generated by moderates and principlists will show how both sides utilized cyberspace to propagate their favored - and directly opposing - political and social agenda through generating and debating different ideational factors associated with political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions.

The conclusion to the dissertation will provide a summary of the research findings and some final remarks.

CHAPTER ONE: LITERATURE REVIEW

Introduction

What is the significance of cyberspace for domestic and global politics that leads states to endeavor to manage it? The literature review for this dissertation draws on existing works to tease out the significance of cyberspace for state-society and international relations and at the same time to discover what parts of the literature exist in regard to the IRI. The academic literature reviewed in this chapter is divided into two broad areas, covering the relationship between state and society at the domestic level and international relations at the global level, respectively, and can be further subdivided to four themes each (Figure 1.1).

The first two themes under state-society relations at the domestic level deal with social mobilization and collective action. The implications of these for states differ depending on where they fall along a spectrum ranging from authoritarian to democratic. For authoritarian states social mobilization poses a special challenge because it carries the potential to undermine the exclusionary basis of such states. Democratic states in contrast tend to be more concerned with collective action arising from criminal and extremist groups which can have a range of deleterious impacts. The third theme deals with the consequence of cyberspace for media coverage. While authoritarian states are concerned about what the cyber domain means for their media monopoly and the possibility of losing it, democracies are concerned with the spread of disinformation, colloquially referred to as “fake news”. The fourth theme deals with the measures taken by states to counter or control the potential of cyberspace in facilitating social mobilization and collective action and generating and framing media coverage. State

propaganda, surveillance and denial of access are the main examples of these measures which are discussed under the fourth theme. The extent to which these measures are deployed differs based on the typology of a state. However, whether authoritarian or democratic, such measures are common among states.

The first theme under international relations is cyber conflict, which can take a myriad of forms. The most common manifestations of cyber conflict include cyber attacks, cyber espionage, and cyber terrorism. The second theme is the economic potential of cyberspace, which affects the very structure of the global economy and the position of each state in the global hierarchy. Given that the economy is considered a source of power in the theoretical framework used in this dissertation, utilizing cyberspace to expand a state's economic power means that it in fact becomes akin to a source of power at the global level. The third theme is the emergence of international organizations, regimes, and norms for global Internet governance. The tension between the non-territorial structure of cyberspace and territorially bounded state sovereignty makes global institutions of Internet governance a necessary locus where state and non-state actors actively engage each other to secure their respective interests. The fourth and final theme linked to international relations deals with ideational factors and the ability they grant states to advance their goals through public diplomacy at an ever faster rate and further reach. Cyberspace provides a whole new domain in which a state can pursue its interests by gathering information about public opinion in a target country and propagating and promoting its policies, political ideals, cultural values, and other ideational factors there. This chapter begins with a brief review of the background, definition and characteristics of cyberspace and then discusses the themes introduced above in detail.

Figure 1.1: The Implications of Cyberspace for State-society and International Relations

1.1. Background: Second Information Revolution

Information revolutions have reshaped human society in fundamental ways. The first information revolution of the nineteenth and twentieth centuries, involving the creation and spread of the telegraph and telephone, radically transformed human society. As Gerald Brock argues, we are now in the midst of a "second information revolution".[34] This ongoing revolution, which has enabled an unprecedented quantity of information to pass through low-cost computers over long distances at

[34] Brock, Gerald W. *The Second Information Revolution*. Cambridge, MA: Harvard University Press, 2003.

rapid speeds, is having an even more transformative effect on human life.[35] Technological advances in the hardware and software that power the centerpiece of the second information revolution, the Internet, happen on an almost daily basis. These rapid advances are captured by three phenomena: the data revolution, rising processing speed of microchips, and ability to send increasingly large volumes of data over optical fiber cables.

We have entered an era of 'Big Data', in which the quantity of data being produced in the world doubles approximately every two years, data which includes everything from records of online purchases, electronic medical files, and posts on social networking sites.[36] This is compounded by Moore's Law, which argues that the processing speed of microchips doubles every 18 months,[37] and Butter's Law of Photonics, which asserts that the amount of data passing through fiber-optic cables doubles every nine months.[38] This means that by 2028, the total amount of global data will be thirty-two times larger, computer processing speeds will be one-hundred times faster, and the volume of data being transmitted across the globe will be more than ten-thousands time larger than it is in 2018. This quantum leap means that humans can communicate, use information and produce knowledge like never before, surmounting limits previously placed on them by location and time.[39]

---

[35] Alberts, David S., and Daniel S. Papp, eds. *The Information Age an Anthology on Its Impacts and Consequences*. Washington, D.C.: CCRP Publication Series, 1997.

[36] Kitchin, Rob. *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. London: Sage, 2014. p.70.

[37] Schmidt, Eric, and Jared Cohen. *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. New York, NY: Knopf Doubleday Publishing Group, 2013. p.5.

[38] Saadoun, Mélissa, and Lin Yanning. "Research, Innovation and Technological Development." *Innovation Engineering: the Power of Intangible Networks*. Ed. Patrick Corsi et al. Newport Beach, CA: ISTE, 2006. 85-104. p. 98.

[39] Dunn Cavelty, Myriam. *Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment*. Zurich: Center for Security Studies (CSS), 2002.

Gerald Brock traces the genealogy of this profound transformation in human society to innovations in information and communications technology as a result of defense projects.[40] Among these, one of the most transformative projects was what later became the Internet, a global system of interconnected computer network. ARPANET, named after the US defense department's Advanced Research Projects Agency (ARPA), was the first version of this network. It went online in 1969. Given its origins as a defense project, the Internet was designed with many redundancies to be resilient against military attack. Unlike the military vulnerable telephone networks it replaced, which relied on a central node to connect correspondents, the Internet uses packet switching which routes messages through several nodes, meaning that it is not reliant on any single node. Janet Abbate asserts that the early Internet "favored military values, such as survivability, flexibility, and high performance," making this network de-centralized and redundant.[41] As citizens began to use the Internet, these qualities also turned out to efficiently facilitate the free flow of information and innovation. Andrew Feenberg and Maria Bakardjieva see these qualities as allowing "creative appropriation", whereby

> Users innovate new functionalities for already existing technologies. Creative appropriation has been a significant shaping force in the evolution of the Internet from the very beginning. It was originally designed for sharing information for the purposes of military research, but users quickly appropriated it as a medium for human communication. Subsequently, the new interpretation was incorporated into the structure of the technology through a series of design changes and now belongs to its accepted social definition.[42]

---

[40] Brock, Gerald W. *The Second Information Revolution*. Cambridge, MA: Harvard University Press, 2003. p.145.

[41] Abbate, Janet. *Inventing the Internet*. Cambridge, Mass: MIT Press, 1999. p.5.

[42] Feenberg, Andrew, and Maria Bakardjieva. "Consumers or Citizens? The Online Community Debate." *Community in the Digital Age: Philosophy and Practice*, Ed. Andrew Feenberg and Darin Barney. Lanham, MD: Rowman & Littlefield, 2004. 1-30. p.16.

These qualities lead many to see the Internet as an inherently participatory medium, which allows an unprecedented, in qualitative and quantitative terms, degree of human interaction to take place. This constitutes the novel characteristic of the second information revolution. While the first information revolution enabled us to strengthen our hold on the existing power domains of land, sea, air, and space, the second information revolution has enabled us to create an entirely new domain for human presence: cyberspace. Modern societies today are strongly dependent on this new domain, or, as Ronald Deibert and Rafal Rohozinski have put it: "They have been locked in and interpenetrated by a digital web of their own spinning".[43] This dependency, which exists at nearly every level from the individual all the way up to supra-national institutions, has been transformative for the theorization and practice of politics.[44] According to Robert Reardon and Nazli Choucri:

> If one defines politics as, at its core, the determination through social relationship of "who gets what, when, how," then the rapid growth of social activity in cyberspace, and the increasing importance of relationships in that domain to international security, the global economy, political and social organization, and the development and spread of ideas, should be seen as potentially transformative.[45]

1.2. Cyberspace: Definition and Characteristics

There is as of yet no universally accepted definition of what cyberspace is. Originally coined in by science fiction writer William Gibson, the term has come to take on multiple meanings.[46]

---

[43] Deibert, Ronald, and Rafal Rohozinski. "Control and Subversion in Russian Cyberspace." *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. Ed. Ronald Deibert et al. Cambridge, MA: MIT Press, 2010, 3–14. p.12.

[44] Castells, Manuel. *The Rise of the Network Society*. Oxford: Blackwell, 1996.

[45] Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." *Explorations in Cyber International Relations*, 1 Apr. 2012, <https://goo.gl/F1kuaK>.p.2.

[46] Gibson, William. *Neuromancer*. New York City, NY: Ace Books, 1984.

Some define cyberspace as a "virtual reality".[47] Others have sought a less abstract and more technical definition, looking at it as a global domain consisting of the "interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[48] Some scholars have emphasized the complex web of social relations as one of the defining aspects of cyberspace. As noted by Ronald Deibert and Rafal Rohozinski, the complex social relations of the mass user base in cyberspace, shaping the domain through its actions and in turn being shaped by it, creates a "dynamic density" that makes the very notion of cyberspace very difficult to pin down.[49] Taking all of these definitions into account, the following definition for cyberspace is proposed here: *a domain made up of the globally connected hardware and software infrastructure and data networks, with the mass user-based complex web of social relations that shapes and is shaped by this domain*.

Cyberspace is not only significant because it is the first man-made power domain, but also because it is the most radically diffusive in terms of power. There are at least three primary reasons why this is the case: low cost of entry, anonymity, and asymmetries in vulnerability.[50] If we place the cost of entry of different power domains side-by-side, we can create a spectrum ranging from the most to least diffusive in terms of power. On one extreme we have the domain of space, where the cost of entry is so high that only a small handful of states and major

---

[47] Heim, Michael. *The Metaphysics of Virtual Reality*. New York: Oxford University Press, 1993.

[48] JCS. "DOD Dictionary of Military and Associated Terms." *Joint Chiefs of Staff*. Mar. 2018. Web. 01 Apr. 2018. <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-03-27-153248-110>. p.60.

[49] Deibert, Ronald, and Rafal Rohozinski. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21.4 (2010): 43-57. p.45.

[50] Nye, Joseph S. *Cyber Power*. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.

corporations with the greatest resources can exercise power there. While the cost of entry into the domain of air is relatively cheaper, air is still to a large extent monopolized by states in terms of the exercise of power. The cost of entry to the power domains of sea and land is relatively much lower than the previous two domains, and as a result exercising power is not limited to a handful of states, but billions of participants. In the words of John Sheldon: “The resources and expertise required to enter, exist in, and exploit cyberspace are extremely modest compared to the resources and expertise required for exploiting land, sea, air and space domains. Anyone with access to networked information-communication technologies can use it.”[51]

Actors in cyberspace also have a unique ability to act anonymously. This constitutes what is known as the ‘problem of attribution’. According to Ryan Kiggins “Cyber operators are able to remain anonymous behind computer screens and keyboards, the only identifying feature of a cyber operator may be the consistencies in software programming that are the telltales of a particular programmer or group of programmers... Threat credibility in cyberspace is undercut by the problem of attribution.”[52] The same spectrum in the same order used in the paragraph above applies here in the context of anonymity: space has the least anonymity of the traditional power domains, while land has the most. However, cyberspace is the most radically anonymous: whereas even on land humans are easily identified by passports, fingerprints, DNA, and other

[51] Sheldon, John B. "The Rise of Cyberpower." *Strategy in the Contemporary World*, Ed. John Baylis, James J. Wirtz, and Colin S. Gray. 4th ed. Oxford: Oxford University Press, 2009. 303-19. p.309.

[52] Kiggins, Ryan David. "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance." *Cyberspace and International Relations: Theory, Prospects and Challenges*, Ed. Jan-Frederik Kremer and Benedikt Müller. Berlin: Springer, 2014. 161-80. p.166.

means, through the use of basic software such as TOR, a change of computer, or an IP address, an actor in cyberspace can avoid detection.[53]

Finally, cyberspace has great asymmetries in vulnerability. In space, air, sea, and land, a state can almost proportionately transform its resources into power. The greater a state's resources, the greater its power. Not so in cyberspace, at least not to the same degree. While a state's resources can be invested to create formidable cyber defenses and offenses, the design of the Internet as an open information network means that the return on investment can be lower here: a single skilled hacker with malicious intent can wreak havoc on a state's critical infrastructure. Something on the same level is difficult to imagine in other power domains. Individuals, while capable of wreaking some havoc on land, sea, air, or space, no matter their resources cannot hope to exercise power in these domains to the same extent as they could in cyberspace.[54] With the above background, definition and characteristics in mind, the following sections review the existing scholarly literature, examining the impact of cyberspace on both state-society and international relations.

1.3. Cyberspace and State-Society Relations

The following subsections examine the major discussions in the academic literature on the significance of cyberspace for state-society relation, dividing them around four main themes: 1) social mobilization 2) collective action 3) generating and framing media coverage and 4) propaganda, surveillance, and denial of access by the state.

---

[53] Chawki, Mohamed. "Anonymity in Cyberspace: Finding the Balance between Privacy and Security." *International Journal of Technology Transfer and Commercialisation* 9.3 (2010): 183-99.

[54] Geers, Kenneth. *Strategic Cyber Security*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2011. p.98.

1.3.1 Social Mobilization in Cyber Era

Commenting on the role of social media during the Iranian Green Movement, Mehdi Yahyanejad and Elham Gheytanchi highlight that "New media lowered the cost of political participation and protest, and proved crucial as the only channels through which large-scale demonstrations could be effectively coordinated down to specifics of date, time and place".[55] This observation demonstrates a crucial way in which cyberspace can impact state-society relations by easing social mobilization through reduced costs. This is because the costs of social mobilization are traditionally high, requiring hierarchical, bureaucratic, and capital and labour intensive organizations to recruit, communicate and coordinate with movements' participants, and to cultivate new resources for advancing the movement's agenda. Cyberspace can radically reduce these costs and thus boost social mobilization.[56]

When it comes to communication for organizing social movements' actions, email and messaging apps in cyberspace make the cost for organizers to reach a mass audience almost zero with virtually no difference in the cost between communicating with one or thousands of people. The same applications enable social movement organizations to interact much more efficiently with their members and sympathizers by giving and receiving feedback in real time. In a similar vein, tools such as online meeting applications and online databases, accessible to multiple users, allow organizers to increase the efficiency of their team efforts and coordination. The cyber-enabled social movement organizations are thus starkly different from the traditional

---

[55] Yahyanedjad, Mehdi, and Elham Gheytanchi. "Social Media, Dissent, and Iran's Green Movement." *Liberation Technology: Social Media and the Struggle for Democracy*. Ed. Larry Diamond and Marc F. Plattner. Baltimor, Md: John Hopkins University Press, 2012. 139-53. p.151.

[56] Garrett, R. Kelly. "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs." *Information, Communication & Society* 9.2 (2006): 202-24.

hierarchical, bureaucratic, and capital and labour intensive organization, instead being relatively decentralized, low-cost, small, and not requiring the spatial and temporal co-presence of the movement's organizers and participants.[57] The latter is of crucial importance for transnational social movements which can hardly be organized in the absence of new information and communication technologies.[58] Analyzing the Iranian Green Movement as a "trans-spatial collective action", Reza Masoudi Nejad shows how leveraging the spatial and temporal co-presence in cyberspace enabled the movement to transcend spatial and temporal barriers and take place in "forty countries, dispersing the protest to about one-hundred-forty cities around the world, from Manila, Dhaka, and Haydarabad, to London, Washington DC, and Los Angeles."[59]

Cyberspace can also enable fast and cheap fundraising by significantly reducing overhead costs, allowing for the efficient collecting of monetary sums. Critically, this includes the mass collection of small sums or 'micro-contributions', which in the past may have been ignored because the cost of collecting them could outweigh the benefits. The benefits of the micro-contributions are not merely financial, but can also be cognitive in that these "small actions may lead to a greater sense of obligation."[60] According to Kelly Garrett, commitment by an individual to a course of action, even if it comes in the form of a micro-contribution, will make that

---

[57] See Karpf's study on MoveOn.org, a low budget, limited staff, and decentralized public policy advocacy group in the United States: Karpf, David. *The MoveOn Effect: The Unexpected Transformation of American Political Advocacy*. New York: Oxford University Press, 2012.

[58] Garrett, R. Kelly. "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs." *Information, Communication & Society* 9.2 (2006): 202-24. p.206.

[59] Masoudi Nejad, Reza. "Trans-spatial Public Action The Geography of Iranian Post-Election Protests in the Age of Web 2.0." *Social Media in Iran: Politics and Society after 2009*, Ed. David M. Faris and Babak Rahimi. Albany: State University of New York Press, 2015. 165-82. p.168.

[60] Garrett, R. Kelly. "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs." *Information, Communication & Society* 9.2 (2006): 202-24.p. 206-7.

individual feel "more committed to the issue and more certain that action was required."[61] Cyberspace thus not only enhances the ability of a social movement organization to reach new sources of funding through the mass-collection of micro-contributions, but also allows it to use this same mechanism to strengthen its bonds with its members and sympathizers.

Not every scholar, however, accepts the notion that cyberspace creates immense cost-reduction and efficiency in communication and coordination efforts. Rasmus Kleis Nielsen underlines how over-communication, miscommunication, and communicative overload can have negative consequences in online communication and coordination efforts, reducing or eliminating the cost-saving benefits of the Internet-assisted activism tools.[62] Drawing on the experience of the 2008 Democratic US presidential primaries, he discovered that campaign organizers felt that the sheer volume and disarray of the online user-generated communication and data was overwhelming, leading them to simply ignore online tools during the most hectic campaign periods. Despite such critiques, the consensus in the literature appears to be that the low-cost of communication and coordination in cyberspace have positive impact on social mobilization, especially given the pace of innovation which leads to the creation of new tools and applications to address the above shortcomings.

Cyberspace has not simply changed the cost-benefit analysis of organizing social movements, but has also done the same for potential participants seeking to join these movements. Before the advent of cyberspace, individuals often had to make a clear, binary, decision on whether or not to

---

[61] Ibid, 207.

[62] Nielsen, Rasmus Kleis. "The Labors of Internet-Assisted Activism: Overcommunication, Miscommunication, and Communicative Overload." *Journal of Information Technology & Politics* 6.3-4 (2009): 267-80.

join a movement, which could entail a varying range of commitment costs. With the advent of cyberspace, however, the initial steps in joining an action or movement as a participant can come at virtually zero cost, ranging from online letter-writing and petitioning, to sharing a link on a social media profile, to donating just tiny contribution.[63] Potential participants thus can engage gradually through small, repeated, low-cost, and low-risk activities as rungs on the 'ladder of engagement' toward maximal offline actions. Once again, some scholars are skeptical about this type of gradualist, low-commitment and low-cost participation in movements, characterizing it as 'slacktivism'. According to Morozov, "'Slacktivism' is an apt term to describe feel-good online activism that has zero political or social impact. It gives those who participate in 'slacktivist' campaigns an illusion of having a meaningful impact on the world without demanding anything more than joining a Facebook group."[64] From this perspective, slacktivism is a worrying trend that can make actions and movements a less powerful force for change because participants have the option to and feel justified in substituting costlier and more effective commitment with less costly and effective online actions.

Rejecting the accusation of slacktivism, however, several studies have found that online activism correlates with offline action suggesting that not only do low-cost online actions not impede offline activism, but on the contrary, the former enhances the level of participants' engagement in

---

[63] Bimber, Bruce, Andrew J. Flanagin, and Cynthia Stohl. "Reconceptualizing Collective Action in the Contemporary Media Environment." *Communication Theory* 15.4 (2005): 365-88.

[64] Morozov, Evgeny. "Foreign Policy: Brave New World Of Slacktivism." *NPR*. 19 May 2009. Web. 01 August 2016. <http://www.npr.org/templates/story/story.php?storyId=104302141>.

the latter type of activism.[65] For instance, Meredith Conroy, Jessica Feezell and Mario Guerrero employed a multi-method design with original survey research of university undergraduates (n = 455) and a content analysis of political group pages online to evaluate the link between membership in an online political group and political engagement as assessed by political participation and knowledge in the context of the 2008 US presidential election.[66] This study found that "participation in online political groups is strongly correlated with offline political participation", suggesting that online activism should be considered as a predictor of offline activism, not its substitute. In the same vein, Ion Bogdan Vasi and Chan Suh show in a study on the Occupy Wall Street movement that online activism on social media platforms such as Facebook and Twitter not only did not lead to slacktivism but positively affected the spread of offline protests with their effect only increasing over time.[67]

Another mechanism through which cyberspace can facilitate social mobilization is the formation and enhancement of social capital. The latter is a term extensively used in various social science disciplines including sociology, economics and political science, highlighting the significant role of resources embedded in the "connections among individuals-social networks and the norms of

---

[65] See: Brunsting, Suzanne, and Tom Postmes. "Social Movement Participation in the Digital Age: Predicting Offline and Online Collective Action." *Small Group Research* 33.5 (2002): 525-54.; Karpf, David. "Online Political Mobilization from the Advocacy Group's Perspective: Looking Beyond Clicktivism." *Policy & Internet* 2.4 (2010): 7-41.; Harlow, Summer, and Dustin Harp. "Collective Action on the Web: A Cross-cultural Study of Social Networking Sites and Online and Offline Activism in the United States and Latin America." *Information, Communication & Society* 15.2 (2012): 196-216.

[66] Conroy, Meredith, Jessica T. Feezell, and Mario Guerrero. "Facebook and Political Engagement: A Study of Online Political Group Membership and Offline Political Engagement." *Computers in Human Behavior* 28.5 (2012): 1535-546.

[67] Vasi, Ion Bogdan, and Chan S. Suh. "Online Activities, Spatial Proximity, and the Diffusion of the Occupy Wall Street Movement in the United States." *Mobilization: An International Quarterly* 21.2 (2016): 139-54.

reciprocity and trustworthiness that arise from them."[68] Cyberspace has enabled the formation of social capital through online social networks, allowing for connections between individuals that transcend temporal and spatial barriers to take shape, while also enhancing social capital by reinforcing connections in existing real-world social networks.[69] The role of cyber networks in enhancing social capital is so significant that Nan Lin, a leading social capital scholar, asserts: "I suggest that indeed we are witnessing a revolutionary rise of social capital, as represented by cyber networks. In fact, we are witnessing a new era in which social capital will soon supersede personal capital in significance and effect."[70]

Based on the strength of the ties within social networks, the academic literature distinguishes between two related but distinct types of social capital: a) Bridging social capital, related to resources available in weak ties (acquaintances); and b) Bonding social capital, related to the resources embedded in strong ties (family, close friends, and trusted associates).[71] Bridging social capital is inclusive and extracted from the relationships of individuals making connections *between* social networks. Although these individuals usually have weak relationships, this is compensated for by the sheer breadth of ties. Dmitri Williams asserts that as a consequence of these characteristics, "bridging may broaden social horizons or world views, or open up

---

[68] Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000. p.19.

[69] Elin, Larry. "The Radicalization of Zeke Spier: How the Internet Contributes to Civic Engagement and New Forms of Social Capital." *Cyberactivism: Online Activism in Theory and Practice*, Ed. Martha McCaughey and Michael D. Ayers. New York: Routledge, 2003. 97-114.

[70] Lin, Nan. *Social Capital: A Theory of Social Structure and Action*. Cambridge, UK: Cambridge University Press, 2001, 214-215.

[71] Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000. p.22.

opportunities for information or new resources."[72] Bonding social capital, however, is exclusive, shaped in the strongly-tied relationships of individuals *within* social networks of family, close friends and trusted associates. While individuals with bonding social capital have limited diversity in their backgrounds, they do have more powerful personal connections. Williams argues that "The continued reciprocity found in bonding social capital provides strong emotional and substantive support and enables mobilization."[73] Pamela Paxton emphasizes that high levels of bridging and bonding social capital result in trusting and reciprocal ties within social networks. This enables social movements to "create and disseminate anti-government discourse" and provide "resources for the organization of opposition movements and large-scale collective action", thereby posing a challenge to the state.[74] This trend is underlined by Nan Lin who views cyber networks as a "revolutionary and powerful means to mobilize capital, social and others, making viable massive social movements even in a most constrained and repressive institutional field. The leaders of the prevailing ideology and institutions correctly recognized these challenges and considered them a serious political struggle."[75] In the same vein, the close observers of Iranian social media during the Green Movement suggest that cyber networks such as Facebook created a new domain of interaction where different forms of bridging and bonding ties could be shaped and expanded. These further emphasize that such ties were "influential in encouraging online discussions, information sharing, news dissemination, and mobilization of

---

[72] Williams, Dmitri. "On and Off the 'Net: Scales for Social Capital in an Online Era." *Journal of Computer-Mediated Communication* 11.2 (2006): 593-628. p.597.

[73] Ibid.

[74] Paxton, Pamela. "Social Capital and Democracy: An Interdependent Relationship." *American Sociological Review* 67.2 (2002): 254-77. p.257.

[75] Lin, Nan. *Social Capital: A Theory of Social Structure and Action*. Cambridge, UK: Cambridge University Press, 2001. p.226.

collective action through ubiquity of access, despite censorship limitations imposed by the Iranian state over the Internet."[76]

In the process of social mobilization, the complex web of weak ties in cyber networks works as an ideal tool for the circulation of information among a critical mass of citizens. This is evident in the findings of a study conducted by the data science team of Facebook. The study suggests that the weak ties generate the majority of information spread and accordingly the bulk of information people consume and share on social network.[77] Acquiring information online can in turn stimulate dialogue and discussion and bolster the rationale for taking collective action.[78] The findings of a study on the use of the internet in the movement against the 2003 US-led invasion of Iraq show that acquiring news and information online drove both face-to-face and online political discussion about the war which in turn had positive links with participation in the anti-war movement.[79] Parallel to the flow of information and rise of shared awareness through weak ties, strong ties within trusting networks of family and friends facilitate the sense of need and possibility of collective action by providing strong emotional and substantive support for that action. Philip Howard and Muzammil Hussain have observed a similar mechanism during the Arab Spring uprisings, highlighting how cyberspace aided Tunisian dissidents to experience a

---

[76] Eloranta, Jari, Hossein Kermani, and Babak Rahimi. "Facebook Iran: Social Capital and the Iranian Social Media." *Social Media in Iran: Politics and Society after 2009*, Ed. David M. Faris and Babak Rahimi. Albany: State University of New York Press, 2015. 19-40. p.21.

[77] Bakshy, Eytan. "Rethinking Information Diversity in Networks." *Facebook*. 17 January 2012. Web. 01 August 2016. <https://www.facebook.com/notes/facebook-data-science/rethinking-information-diversity-in-networks/10150503499618859/>.

[78] Shah, Dhavan V., Jaeho Cho, William P. Eveland JR., and Nojin Kwak. "Information and Expression in a Digital Age: Modeling Internet Effects on Civic Participation." *Communication Research* 32.5 (2005): 531-65.

[79] Nah, Seungahn, Aaron S. Veenstra, and Dhavan V. Shah. "The Internet and Anti-War Activism: A Case Study of Information, Expression, and Action." *Journal of Computer-Mediated Communication* 12.1 (2006): 230-47.

sense of common grievances within networks of family and friends through their shared sympathy with Mohamed Bouazizi, the street vendor who lit himself on fire as an expression of frustration with the social and political status-quo.[80]

The above are the major mechanisms through which cyberspace facilitates social mobilization. In chapter three we will examine the coercive measures the IRI undertakes to control or counter these mechanisms.

1.3.2. Cyberspace and Collective Action Repertoires

Another mechanism through which cyberspace can impact state-society relations is the optimization and expansion of tactics adopted by social movements, or what Tilly called social movements' "repertoires of contention".[81] According to Jennifer Earl and Katrina Kimport, the concept of repertoires of contention was introduced by Tilly to "capture the set of tactical forms from which social movement actors can choose at any given historical moment as well as denote the common characteristics shared by the set of available tactical forms in a historical moment."[82] The changes to social movements' repertoires of contention in the cyber era can be formulated in academic literature through two main categories: cyber-assisted and cyber-based repertoires.

---

[80] Howard, Philip N., and Muzammil M. Hussain. "The Role of Digital Media." *Democratization and Authoritarianism in the Arab World*, Ed. Larry Diamond and Marc F. Plattner. Baltimore: Johns Hopkins University Press, 2014. 186-99. p.187.

[81] Tilly, Charles. "Repertoires of Contention in America and Britain, 1750-1830." *The Dynamics of Social Movements: Resource Mobilization, Social Control, and Tactics*, Ed. Mayer N. Zald and John D. McCarthy. Cambridge, MA: Winthrop Publishers, 1979. 126-55.

[82] Earl, Jennifer, and Katrina Kimport. *Digitally Enabled Social Change: Activism in the Internet Age*. Cambridge, MA: MIT Press, 2011. p.16.

In the first category cyberspace does not provide the activists with new repertoires, but instead enhances the efficiency of already available ones by reducing the cost and increasing the speed, reach and size of the collective action. In this sense, social movement organizations can make extensive use of cyberspace to enhance fundraising and coordination efforts for mobilizing national and transitional demonstrations.[83] This is documented in a plethora of case-studies, including the Zapatista movement,[84] anti-globalization movement,[85] transnational protest against the Iraq war in 2003,[86] Arab Spring demonstrations,[87] and Iranian Green Movement.[88] Some scholars also contend that cyber-assisted tactics allow for the fast dissemination of information about the time and location of collective actions, helping social movement activists to reduce the possibility of surveillance and repressive response by the security forces.[89] For instance, in the 2010 student demonstrations in London, the protesters used the Sukey network based on Google

---

[83] Van Laer, Jeroen. "Activists “online” and “offline”: Internet as an Information Channel for Protest Demonstrations." *Mobilization: An International Journal* 15.3 (2010): 405-21.

[84] Cleaver, Harry M. "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric." *Journal of International Affairs* 51.2 (1998): 621-40.

[85] Van Aelst, Peter, and Stefaan Walgrave. "New Media, New Movements? The Role of the Internet in Shaping the ‘anti-globalization’ Movement." *Cyberprotest: New Media, Citizens and Social Movements.* Ed. Wim Van De Donk, Brian D. Loader, Paul G. Nixon, and Dieter Rucht. London: Routledge, 2004. 87-108; Eagleton-Pierce, Matthew. "The Internet and the Seattle WTO Protests." *Peace Review* 13.3 (2001): 331-37.

[86] Bennett, W. Lance, Christian Breunig, and Terri Givens. "Communication and Political Mobilization: Digital Media and the Organization of Anti-Iraq War Demonstrations in the U.S." *Political Communication* 25.3 (2008): 269-89.

[87] Howard, Philip N., and Muzammil M. Hussain. *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. Oxford: Oxford University Press, 2013.

[88] Sadeghi Esfahani, Mohammad. "The Politics and Anti-Politics of Facebook in Context of the Iranian 2009 Presidential Elections and Beyond." *Social Media in Iran: Politics and Society after 2009*. Ed. David M. Faris and Babak Rahimi. Albany, NY: State University of New York, 2016. 137-64.; Masoudi Nejad, Reza. "Trans-spatial Public Action The Geography of Iranian Post-Election Protests in the Age of Web 2.0." *Social Media in Iran: Politics and Society after 2009*. Ed. David M. Faris and Babak Rahimi. Albany, NY: State University of New York, 2016. 165-82.

[89] McPhail, Clark, and John D. McCarthy. "Protest Mobilization, Protest Repression and Their Interaction." *Repression and Mobilization*, Ed. Christian Davenport, Hank Johnston, and Carol Mueller. Minneapolis: University of Minnesota Press, 2005. 3-32.

Maps and mobile phones to not get trapped, or “kettled”, by the police. During demonstrations, the Sukey network team collected information from protesters’ tweets, texts and GPS positions then updated an online live-map of the protest that protesters could access through their smartphones. At the same time, “they tweet and text brief summaries of events to all their subscribers, telling them where other protesters are situated, and - most significantly - where kettles are forming.”[90]

At another level, activists use cyberspace to develop new tactics enabled by and based within this domain, including online petitions and hacktivism (a portmanteau of hack and activism). A good example of successful online petitioning is *MoveOn.org*, which began as an online petition opposing the impeachment of Bill Clinton in 1998 that 500,000 people ultimately signed, and has since hosted numerous other petitions, including a petition against the Iraq war in 2003 that collected 220,000 signatures. Petitioning web sites, such as *Petitiononline.com*, have hosted tens of thousands of petitions and collected more than 33 million signatures.[91] Moreover, cyberspace with its unique media capabilities, has facilitated new forms of petitioning such as visual petitions. People sign on to these petitions by uploading a picture of themselves that often displays a personal message. An illustrative example of visual petitioning in the Iranian context is the ‘Men wearing Hijab’ campaign to support Majid Tavakoli, one of the leading figures of the Iranian student movement. Tavakkoli became a student symbol of the Green Movement on Iranian Student Day when security forces sought to humiliate him by claiming he had tried to

---

[90] Kingsley, Patrick. "Inside the Anti-kettling HQ." *The Guardian*. 02 February 2011. Web. 02 August 2016. <https://www.theguardian.com/uk/2011/feb/02/inside-anti-kettling-hq>.

[91] Earl, Jennifer. "Pursuing Social Change Online: The Use of Four Protest Tactics on the Internet." *Social Science Computer Review* 24.3 (2006): 362-77.

escape arrest by donning the veil and pretending to be a woman. Rather than discrediting him, this turned Tavakkoli into a social media phenomenon, with hundreds of men uploading photos of themselves in the veil to demonstrate solidarity with him, ask for his release, and raise objections to the practice of forced veiling of women in Iran.

Cyberspace has also created a new space for hacktivism which refers to a broad range of confrontational online activities including virtual sit-ins or Distributed Denial of Service (DDoS) attacks, Domain Name System (DNS) hijacking or redirection, and website defacements. Based on different viewpoints, these tactics can be categorized as legal or illegal and thus placed on a broad spectrum from 'electronic civil disobedience' to 'cyberterrorism'.[92] Virtual sit-ins or DDoS attacks involve large numbers of people sending repeated simultaneous requests to target websites to make them inaccessible to visitors. The high number and simultaneous requests overload the website server to the extent that it ceases to process requests and eventually becomes unavailable to its intended visitors. This tactic was used during the Green Movement demonstrations when activists used page reboot applications to mount DDoS attacks to bring down the website of the supreme leader, the president, and state and quasi-state media outlets such as Islamic Republic of Iran Broadcasting (IRIB) and Fars News Agency.[93] Another tactic is DNS hijacking or redirection, in which a hacker alters the source code of a website in order to reroute visitors to other websites. In July 1998, for instance, an international group of hackers attacked some 300 websites to redirect the audience of the victim websites to their own websites,

---

[92] Laer, Jeroen Van, and Peter Van Aelst. "Internet And Social Movement Action Repertoires." *Information, Communication & Society* 13.8 (2010): 1146-171. p.1159.

[93] Sreberny, Annabelle, and Gholam Khiabany. Blogistan: *The Internet and Politics in Iran*. London: I.B. Tauris, 2010. p.176.

which consisted of content protesting against the nuclear arms race. Website defacement is another tactic in which a hacker leaves a message or cover photo on the homepage of the victim's website to protest or support a particular cause. In 2003, for instance, over 10,000 websites were defaced by different hacker groups, most of them protesting against the US-led invasion of Iraq, while some supported the war.[94]

Jeroen Van Laer and Peter Van Aelst offer a two-dimensional typology for understanding how cyberspace transformed social movements' repertoires of contention (see figure below), covering the wide range of tactics available to individuals.[95] Similar to the dichotomy presented above, the first dimension shows the spectrum of tactics from internet-supported to internet-based tools, with the former enhancing already existing tactics not native to cyberspace and the latter expanding social movements' repertoires of contention by offering novel tactics only possible online. The second dimension shows the spectrum of low- to high-threshold tactics, with low-threshold tactics requiring limited effort, commitment, or risk, whereas high-threshold tactics can entail much greater ardor, commitment and risk. This typology covers the wide range of social movements' repertoires of contention, while responding to the common critique that cyberspace only promotes low-threshold activities. The authors show cyberspace can in fact enable high-threshold activities, and that even low-threshold activities can be viewed as just the first step towards more high-threshold ones (Figure 1.2).[96]

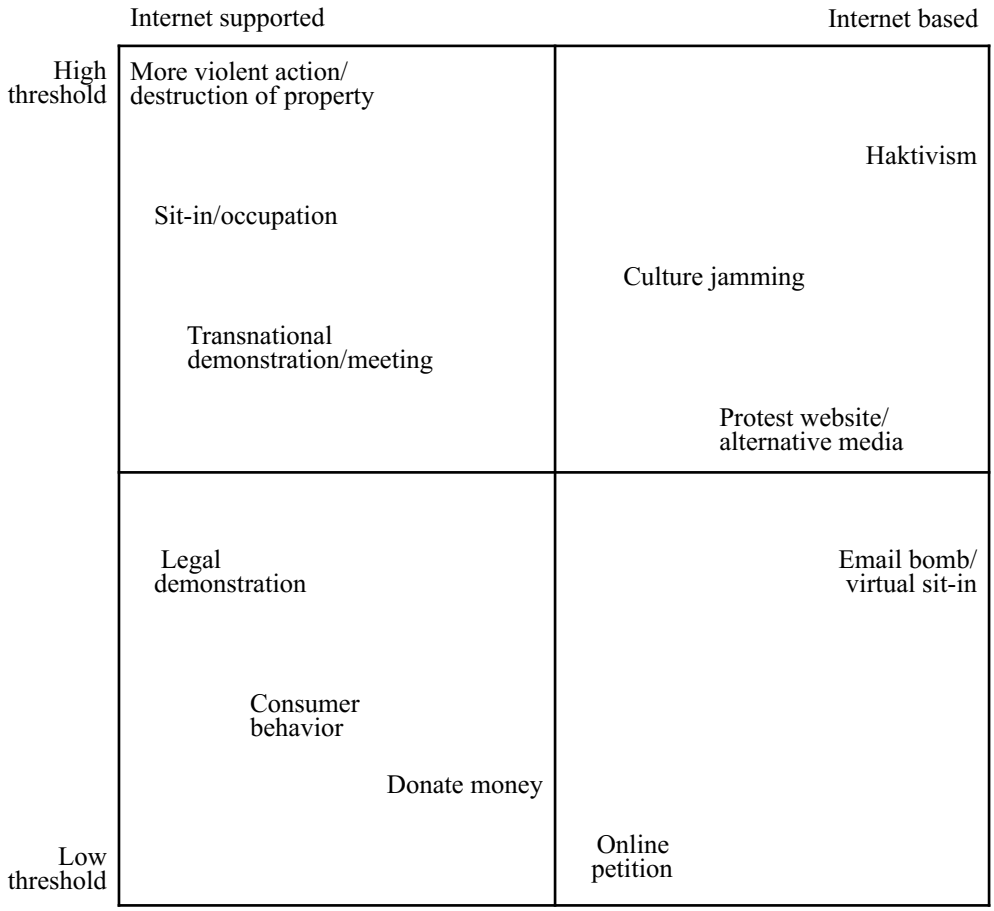
---

[94] Laer, Jeroen Van, and Peter Van Aelst. "Internet And Social Movement Action Repertoires." *Information, Communication & Society* 13.8 (2010): 1146-171. p.1160.

[95] Ibid.

[96] Ibid. p.1149.

Figure 1.2: A Typology of a New Digitalized Action Repertoire



This subsection reviewed how cyberspace enables social movements to optimize and expand the tactics they adopt for contestation with the state. We will study the IRI's coercive measures to counter this in chapter three.

1.3.3. Generating and Framing Media Coverage in Cyberspace

Another way cyberspace can critically impact social movements is to generate and frame media coverage. According to R. Kelly Garrett, framing media coverage can be defined as "strategic attempts to craft, disseminate and contest the language and narratives used to describe a movement. The objective of this process is to justify activists' claims and motivate action using

culturally shared beliefs and understandings."[97] A vast body of academic literature on social movements has been devoted to the framing processes, underscoring that without effective framing that resonates with would-be participants and supporters, a social movement's mobilization potential cannot be realized. Following the work of Robert M. Entman, a resonant frame can be viewed as a schemata for the organization and interpretation of information to influence people, and is based on the following four main pillars: 1) problem definition or determining the problem under consideration; 2) causal interpretation or identifying the forces creating the problem; 3) moral evaluation or judging the causal agents and their effects; 4) treatment recommendation or offering treatments for the problems and predicting their potential effects.[98]

In the processes of generating and framing media coverage, social movements were historically dependent on corporate or state-owned mass media which would often show bias towards authorities in power and established institutions, and tend to remain silent about, or distort the message of, a social movement, highlighting its disruptive and violent aspects instead.[99] In the cyber era, however, social movements can leverage what Emanuel Castle calls "mass self-communication", or the ability of the masses to self-generate and self-direct messages to a global audience en masse.[100] This leverage provides social movements with the opportunity to generate and frame media coverage by bypassing, indirectly accessing, and even influencing mass media. Occupy Wall Street is an illustrative example of a social movement aptly using mass self-

---

[97] Garrett, R. Kelly. "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs." *Information, Communication & Society* 9.2 (2006): 202-24. p.204.

[98] Entman, Robert M. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43.4 (1993): 51-58.

[99] Della Porta, Donatella, and Mario Diani. *Social Movements: An Introduction*. 2nd ed. Malden, MA: Blackwell Publishing, 2006.

[100] Castells, Manuel. *Communication Power*. Oxford: Oxford University Press, 2009.

communication tactics. Kevin M. Deluca, Sean Lawson and Ye Su show that while the movement was initially neglected and ultimately frivolously framed by mass media, it was still able to generate and frame media coverage using online platforms and application for blogging, social networking and mass e-mailing.[101] Analyzing public opinion poll data, the authors further highlight that these tactics adopted by the Occupy Wall Street were quite successful in spreading the movement's news, promoting its narrative and educating the public about the rise of economic inequality in the United States.

Generating and framing media coverage is even more challenging in countries where mass media is largely monopolized by the state. In such contexts, cyberspace is virtually the only public participatory space to generate and frame media coverage challenging the state's ideological and hegemonic structures. During the Green Movement demonstration in Iran, for example, the movement's main leaders published a number of communiqués and manifestos on websites such as *Kaleme* and *Saham News* to create and circulate their messages and viewpoints among the public. Moreover, while foreign media was forced to leave the country and domestic mass media was framing the movement as a foreign backed sedition, platforms such as Facebook, Twitter, and YouTube became key tools for the Green Movement to frame itself as a non-violent, pro-democracy, civil rights movement and disseminate news about the harsh suppression meted out by the security forces.[102] This battle over framing played out in a number of incidents, for example when Iranian state television broadcast pictures of property damage in Tehran and

---

[101] Deluca, Kevin M., Sean Lawson, and Ye Sun. "Occupy Wall Street on the Public Screens of Social Media: The Many Framings of the Birth of a Protest Movement." *Communication, Culture & Critique* 5.4 (2012): 483-509.

[102] Safshekan, Roozbeh. "The Matrix of Communication in Social Movements: A Comparison of the 1979 Revolution and 2009 Green Movement in Iran." *Sociology of Islam* 2.3-4 (2014): 328-45.

elsewhere to frame demonstrators as just a small handful of seditious rebels and vandals. In response, demonstrators uploaded videos of their own that underscored the peaceful nature of their movement and its multitude of participants. What's more, they also uploaded videos that showed how security forces, by wantonly damaging buildings and cars, had perpetrated the very property damage they had accused the Green Movement of creating. The most powerful instance of the Green Movement demonstrators generating and framing media coverage was the mobile phone video of the death of Neda Agha-Soltan uploaded to YouTube.[103] This graphic video, showing Agha-Soltan bleeding to death, went viral, providing "the Green Movement with a powerful symbol of worldwide resonation, representing the struggle of nonviolent young protesters against a repressive state."[104]

Although cyberspace provides social movements with significant opportunities for generating and framing media coverage against the state, the latter often subsequently strike back by utilizing this very domain to limit and even reverse this trend. This is illustrated in the findings of Marcus Michaelsen on reformist online journalism in Iran in the 1997-2005 period. The author argues that after the principlist (conservative) elite in Iran restricted the reform movement's access to mass media, reformists utilized cyberspace as an alternative media space to generate and frame media coverage. The state, however, attempted to reverse this trend through "censorship, surveillance, and the persecution of online dissidents," as well as "the discursive "occupation" of online space by various news media tied to conservative and hardline groups."[105]

---

[103] Sabety, Setareh. "Graphic Content: The Semiotics of a YouTube Uprising." *Media, Power, and Politics in the Digital Age: The 2009 Presidential Election Uprising in Iran*, Ed. Yahya R. Kamalipour. Lanham, MD: Rowman & Littlefield Publishers, 2010. 119-24.

[104] Michaelsen, Marcus. "The Politics of Online Journalism in Iran." *Social Media in Iran: Politics and Society after 2009*. Ed. David M. Faris and Babak Rahimi. Albany, NY: State U of New York, 2015. 101-22. p.104.

[105] Ibid. p.116.

By exploiting the characteristics of cyberspace, "the Iranian Principalists found on the Internet an additional and flexible channel to access public discourse and propagate their interpretations of reality."[106] This trend is further discussed in two chapters of this dissertation. Chapter three shows the attempt by principlists to preserve their monopoly over the Iranian media ecosystem using coercion. Chapter six touches on the use of cyberspace by principlist governmental officials and public figures to propagate their ideas.

1.3.4. Propaganda, Surveillance, and Denial of Access by State

The emancipatory potential of novel information and communication technologies has been well-documented by the academic literature, which has shown how technologies like the printing press, telephone and radio were initially used by the public to challenge state authority. However, in time states counter by utilizing the very same technologies as tools of "propaganda, surveillance, and subjugation".[107] The same is true for cyberspace. Social movement activists are not the only ones utilizing cyberspace to change the balance of power vis-a-vis the state in their favor. Cyberspace can also be used by states to reverse this trend, centralizing power in their hands at the expense of social movements. As Daniel Bell foresaw in the late 1970's, well before cyberspace became a fact of daily life: "the new revolution in communications makes possible both an intense degree of centralization of power, if the society decides to use it in that way, and large decentralization because of the multiplicity, diversity, and cheapness of the modes of communication".[108] In line with Ronfeldt and Varda's observation, the main mechanisms

[106] Ibid.

[107] Ronfeldt, David, and Danielle Varda. "The Prospects for Cyberocracy (Revisited)." *Social Science Research Network (SSRN)*. 01 Dec. 2008. Web. 01 August 2016. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1325809>.

[108] Ibid. p.30.

enabling states to centralize power over society can be categorized as propaganda, surveillance and access denial.

When it comes to promoting and framing ideas, the state can actively utilize cyberspace to propagate its own ideas. This has been observed in studies on the Chinese government's virtual army of state-funded online commentators. Colloquially referred to as the "fifty cent army", these commentators participate in anonymous online discussions on a variety of platforms to create a steady stream of content favorable to the ruling system.[109] In the Iranian context, the Islamic Revolutionary Guard Corps (IRGC) managed to generate 10000 blogs, while the Bureau for the Developments of Religious Web Logs actively promotes the use of cyberspace among the clergy in order to generate and disseminate content in line with the IRI's social, political and cultural ideals.[110] In his analysis of the politics of the Internet in Iran, Babak Rahimi underlines that: "The Internet, according to several clerics, is a "gift to spread the word of the prophet," and its potential benefit for Islam is immeasurable…The state-sponsored religious centers in the conservative cities of Mashhad and Qom have been busy building websites, and providing their interpretation (tafsir) of the Quran on their homepages."[111] The propagation of the IRI's favored political ideals, cultural values, and other ideational factors will be further examined in chapter six.

On the other hand, cyberspace has significantly enhanced state surveillance capabilities by lowering the cost of monitoring information and communication. This has made it much more

---

[109] Han, Rongbin. "Defending the Authoritarian Regime Online: China's "Voluntary Fifty-cent Army"." *Journal of Current Chinese Affairs* 44.2 (2015): 105-34.

[110] Howard, Philip N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford: Oxford University Press, 2010. p.4.

[111] Rahimi, Babak. "The Politics of the Internet in Iran." *Media, Culture and Society in Iran: Living with Globalization and the Islamic State*, Ed. Mehdi Semati. London: Routledge, 2008. 37-56. p.43.

straightforward for states to surveil social movements and detect and punish activists and, as a direct consequence, to "anticipate and regulate civic protest."[112] An ancillary consequence, distinct but related to state surveillance and protest regulation, has been to create a climate of self-censorship on the part of users out of fear of state reprisal.

The revelations about the comprehensive and expansive digital surveillance practices conducted by the United States National Security Agency (NSA) illuminate the potentially insidious ways in which cyberspace can be used to collect, analyze, and store vast amount of data by the government agencies. Citing a former NSA employee who left the agency in protest, Ronald Deibert estimates that "up to 1.5 billion phone calls, as well as voluminous flows of email and other electronic data, are processed every day."[113] This seems to be the realization of a nightmarish scenario that commentators such as David Burnham warned about long ago, emphasizing that the increased powers of surveillance enabled by new information and communication technologies would lead to the "The Rise of the Computer State" capable of conducting centralized state surveillance as envisioned by George Orwell's 1984.[114] Chapter three underlines this trend in Iranian cyberspace and shows how the National Information Network (NIN), alongside other pillars of coercion, can facilitate the IRI's ability to surveil Iranian society and compromise the online security of users.

Finally, states are capable of imposing a comprehensive regime of filtering consisting of "a phalanx of laws and technical measures" to deny users access to certain information online.

---

[112] Drezner, Daniel W. "Weighing the Scales: The Internet's Effect On State-Society Relations." *The Global Flow of Information: Legal, Social, and Cultural Perspectives*. Ed. Ramesh Subramanian and Eddan Katz. New York: New York UP, 2011. 121-38. p.129.

[113] Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013. p.42.

[114] Burnham, David. *The Rise of the Computer State*. New York: Random House, 1983.

Under such a regime, Internet choke points such as large Internet service providers (ISPs) are manipulated to integrate keywords, domains, and/or lists of Internet protocol (IP) addresses, into routers and software in order to deny users within the targeted jurisdiction access to information.[115] According to the 2012 Internet filtering ranking published by OpenNet Initiative, China and Iran have the most restrictive regime of filtering among the 74 studied countries, which also included Pakistan, Saudi Arabia, Turkey and Syria.[116] Filtered content usually includes anti-state political websites, content challenging social norms and morals promoted by government, websites belonging to armed rebel groups, extremists and terrorists, and websites providing users with intermediary applications, such as anonymizers and circumvention tools that allow access to or enable sharing of sensitive information. Chapter three investigates the ways in which the comprehensive regime of filtering denies the user access to information online. While the literature dealing with online access denial often focuses on filtering, chapter three also delves into how the restrictive body of law regulating cyber activities and the main law enforcement organizations created for its implementation deter access to select online information through not only coercion but also self-regulation by Iranian users due to the fear of punishment.

However, some scholars argue that a state's ability to deny access to the Internet is limited by economic barriers. This is encapsulated by the classic "dictator's dilemma" faced by repressive states: "in order to reap the economic rewards offered by adopting information technologies, they

---

[115] Zittrain, Jonathan, and Rafal Rohozinski. "Internet Filtering: The Politics and Mechanisms of Control." *Access Denied: The Practice and Policy of Global Internet Filtering*, Ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: MIT Press, 2008. 29-56. p.32.

[116] Rininsland, Ændrew. "Internet Censorship Listed: How Does Each Country Compare?" *The Guardian*. 16 April 2012. Web. 06 August 2016. <https://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list>.

must accept the political risks these same technologies present."[117] The tradeoff between the economic benefits of cyberspace versus maintaining political control forces even highly authoritarian states to accept at least a minimal level of openness in cyberspace. But even if states are willing to ignore the economic opportunity costs of denial of access, they are faced with a host of real costs because it entails significant technical and economic resources given the proliferation of circumvention tools. To give only one example, China's Golden Shield Project, the official name of the Chinese filtering regime many call the "Great Firewall of China", cost a total of RMB ¥ 8.4 billion (approximately US $ 1.23 billion) in just its first five years of existence from 1998 to 2003.[118] This is consistent with the findings of John Kelly and Bruce Etling's analysis of Iran's online public: "In Iran, satellite TV, Internet based radio stations, cell phones, and other Internet based tools are difficult if not impossible for the regime to control. Costs are generally high for regimes that limit access and connectivity. The Internet will not lead automatically to liberal, open public spheres in authoritarian regimes, but it will make it harder to control and more costly for authoritarian states to do so."[119] Chapter three looks at how the IRI has tried to manage the "dictator's dilemma" while also engaging in access denial using the National Information Network (NIN). This Iranian intranet can be used by the IRI to engage in access denial when it deems it necessary without paying a large economic price because the NIN can continue to operate even when access to the global Internet is denied.

---

[117] Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." *Explorations in Cyber International Relations*, 1 Apr. 2012, <https://ecir.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf>.

[118] Zixue, Tai. "The Great Firewall." *The Internet in China: Cultural, Political, and Social Dimensions,1980s-2000s*, Ed. Ashley Esarey and Randy Kluver. Great Barrington: Berkshire Publishing Group, 2014. 64-74.

[119] Kelly, John, and Bruce Etling. "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere." *The Berkman Klein Center for Internet & Society at Harvard University*. April 2008. Web. 07 Apr. 2018. <https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf>.

1.4. Cyberspace and International Relations

In the previous sections of this chapter, we focused on the impact of cyberspace at the domestic level on the relationship between state and society. In the following sections, we will switch to the global level and look at the impact of cyberspace on international relations that lead states to endeavour to manage it as an emerging domain of power. The major discussions in the academic literature on the significance of cyberspace for international relations are clustered and examined around the four following themes: 1) international security, 2) global economy, 3) global cyber governance, and 4) public diplomacy.

1.4.1 New Challenges to International Security in Cyber Era

One channel through which cyberspace impacts global politics is through the new challenges it poses on international security, specifically in the form of two belligerent actions: cyber espionage and cyber war.[120]

Cyber espionage can serve the function of extracting sensitive and protected information, either for the purpose of industrial espionage or to obtain government secrets. According to existing estimates, cyber industrial espionage costs the US economy $300 billion annually,[121] Germany $28-71 billion and South Korea $82 billion, while 86 percent of large Canadian corporations had been victims of cyber industrial espionage at some point.[122] Industrial espionage through

---

[120] Clark, David, Thomas Berson, and Herbert Lin, eds. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC: National Academies, 2014.

[121] IP. "The Report of the Commission on the Theft of American Intellectual Property." *The IP Commission*. May 2013. Web. 07 August 2016. <http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf>.

[122] ONCE. "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011." *Office of the National Counterintelligence Executive*. October 2011. Web. 07 August 2016. <https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf>.

cyberspace can take many forms and impact a wide facet of global commerce, but the most typical is theft of proprietary information, especially intellectual property, with at least two major consequences. First, theft of proprietary information through cyberspace allows an actor to forgo research and development or patent licensing costs associated with obtaining intellectual property, also allowing it to gain an unfair competitive advantage by creating products more efficiently. Second, theft of proprietary information in the form of insider knowledge can give an actor leverage in negotiations or transactions by gaining insight into an individual or organization's thinking and future plans. The current academic literature shows that China is among the countries that have extensively used industrial espionage in its quest to modernize and grow its economy.[123]

Cyber espionage for the purpose of obtaining state secrets is equally important and pervasive. In 2008, sensitive information belonging to the US Department of Defense was significantly compromised after allegedly Russian spyware was inserted into a US military laptop at a base in the Middle East through a flash drive. The spyware gained access to the US Central Command computer networks, causing arguably "the most significant breach of US military computers ever."[124] In 2014, a similarly spectacular hack against the US Office of Personnel Management saw up to 22 million records of current, former and prospective federal employees, contractors, and security clearance seekers stolen, opening the government and individuals affected to a range of vulnerabilities.[125]

---

[123] Hannas, Wm C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*. New York: Routledge, 2013; Inkster, Nigel. "Chinese Intelligence in the Cyber Age." *Survival: Global Politics and Strategy* 55.1 (2013): 45-66; Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford: Oxford University Press, 2015.

[124] Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89.5 (2010): 97-108.

[125] Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016. p.115.

In 2009, researchers of the Citizen Lab at the University of Toronto discovered an espionage network, dubbed GhostNet, targeting 103 countries and critical ministries, embassies, government agencies, international media, and high-value individuals. The targeted countries and international institutions included Iran, Indonesia, India, South Korea, Indonesia, Romania, Thailand, Taiwan, Portugal, Germany, Pakistan, the United Nations, ASEAN, and NATO. Thought to have come from Chinese cyberspace, subsequent research has apparently confirmed China's involvement.[126] Finally, the Edward Snowden leaks in 2013 indicated that the NSA was able to gain access to sensitive information by hacking Tsinghua University in Beijing, the site of one of mainland China's six "network backbones" routing all of its Internet traffic, as well as the headquarters of Pacnet in Hong Kong, among the largest fiber-optic network operators in the Asia-Pacific.[127]

Although cyber espionage is a very pervasive form of belligerent cyber action, the story does not end here. A second, and arguably more destructive, form of belligerent cyber action can sabotage information systems, and has the potential to create such havoc that some have gone as far as calling it 'cyber war'. The first articulation of cyber war in academic literature was in a book chapter entitled "Cyberwar is coming!" by John Arquilla and David Ronfeldt. According to the authors: "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles."[128] Based on this definition, cyberwar consists of actions for

---

[126] Deibert, Ronald, and Rafal Rohozinski. "Tracking GhostNet: Investigating a Cyber Espionage Network." *Information Warfare Monitor*. 29 March 2009. Web. 07 August 2016. <https://citizenlab.org/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/>.

[127] Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014. p.140.

[128] Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" In *In Athena's Camp Preparing for Conflict in the Information Age*, by John Arquilla and David Ronfeldt, 23-60. Santa Monica: RAND Corporation, 1997. p.30.

disrupting the information and communications systems on which an adversary relies in order to conduct war. By changing the balance of information in a military context, the actor that wins this war can save capital and labor to win the actual war. This definition is among the earliest and most influential articulations of cyberwar, highlighting the potentials of cyberspace in information operations for disrupting the adversary's information systems. Among the examples of this articulation of cyber war is Operation Orchard by the Israeli air force in 2007, which bombed a nuclear facility in Syria's Deir ez-Zor region. Prior to the bombing run, Israel was able to hack and disable the Syrian air defense system, preventing it from detecting and responding to incoming Israeli aircraft. Although the details of this operation remain classified, it can nonetheless be said with high level of certainty that the cyber element of this operation was critical to its success.[129]

However, as states have become more sophisticated in conducting cyber operations, this articulation of cyber war, referred to as tactical information operations, highlights just one aspect of belligerent cyber action, ignoring the use of cyberspace for conducting strategic attacks on critical infrastructure.[130] Addressing this shortcoming, Arquilla revisited his earlier articulation of cyberwar acknowledging that in their earlier contribution they "played down the idea of using cyberspace-based attacks strategically; that is, in a manner akin to aerial bombardment of an adversary's homeland infrastructures."[131] Arquilla pointed out that incidents such as Stuxnet attack against Iranian uranium enrichment centrifuges proved that cyberspace is not merely used

---

[129] Tabansky, Lior, and Isaac Ben-Israel. *Cybersecurity in Israel*. London: Springer, 2015. p.65.

[130] Hakim, Simon, and Robert M. Clark, eds. *Cyber-physical Security: Protecting Critical Infrastructure at the State and Local Level*. Switzerland: Springer, 2017.

[131] Arquilla, John. "Twenty Years of Cyberwar." In *Military Ethics and Emerging Technologies*, by Timothy J. Demy, George R. Lucas, Jr., and Bradley J. Strawser, 275-82. New York: Routledge, 2014. p.275.

for tactical information operations but could also clearly be utilized for strategic attacks with "destructive purposes in the 'real world.'"[132] It is believed that in the Stuxnet strategic destructive operation in 2010, a computer worm custom designed by state actors who many believe to be the United States and Israel, was transmitted to the Natanz uranium enrichment facility through a flash drive. From there, the worm was able to take control of the Siemens industrial control systems and cause Iranian centrifuges to continually speed up and slow down, with the ultimate effect of physically destroying infected centrifuges.[133] The Stuxnet attack signalled Iran's status as being among the first victims of a major cyber attack in the world and led it to take defensive and offensive measures to establish deterrence against its foreign adversaries. Chapter three, which details the Stuxnet attack and all subsequent major cyber attacks on Iran, is the first comprehensive account of these measures.

The realization that contemporary cyberwar encapsulates both tactical information operations and strategic destructive operations has led scholars to seek new definitions of cyberwar. For instance, Richard A. Clarke and Robert Knake define cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[134] In the same vein, Joseph Nye defines cyberwar as "hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence."[135] Some scholars, however, think that offensive destructive actions in cyberspace should not be considered as acts

---

[132] Ibid. p.276.

[133] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.

[134] Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York, NY: Harper Collins, 2010. p.6.

[135] Nye, Joseph S. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter (2011): 20-38.

of war. Drawing upon Clausewitz's definition of war, Thomas Rid argues that war needs to fulfill three main criteria. First, Rid asserts that war has a violent character: "A real act of war is always potentially or actually lethal, at least for some participants on at least one side."[136] Second, war has an instrumental character in which violence is used as a means to compel the enemy to act according to one's own end. Finally, war has a political character, in which the ends to which violence is a means should have a political motive. Based on these criteria, Rid argues that cyber-attacks fail to meet the standards of war, specifically because they do not result in violence and casualties, and are unlikely to do so in the future. Moreover, cyber war does not meet the instrumental and political criteria of war because of the issue of attribution, with Rid arguing that for an act of violence to meet this criteria, it has to be "attributed to one side at some point during the confrontation. History does not know acts of war without eventual attribution."[137]

Rid's arguments for not classifying cyber-attacks as an act of war have been countered by some scholars. Regarding the issue of the lethal and violent characteristic of war, critiques of Rid argue that cyber attacks can have consequences which in fact lead to injuries and loss of life, and thus have the potential for violence. In order to define a cyber-attack as war, Gary McGraw sees the violent characteristic of war as simply requiring a consequential kinetic effect in which there needs to be a physical impact.[138] McGraw uses the infection of Iranian uranium enrichment facilities by the Stuxnet worm, and the resulting physical damage to centrifuges, as an example of a cyber-attack resulting in a kinetic effect. Furthermore, while cyber-attacks may not yet have

---

[136] Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35.1 (2012): 5-32. p.7.

[137] Ibid. p.8.

[138] Mcgraw, Gary. "Cyber War Is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36.1 (2013): 109-19.

direct lethal potential, given the pace of technological change we may very well see such capabilities emerge in the near future. Other scholars have taken issue with Rid's requirement of attribution as part of the Clausewitzian definition of war. They have argued that Clausewitz never saw attribution as a criterion for what constituted war. Moreover, just because cyber wars of the present have not been claimed and attributed does not mean that they will not be in the future.[139] Given the complexities of modern cyber-attacks, attribution has become more feasible, in terms of narrowing down the list to the usual suspects, and may become more prominent in the cyber wars of the future.[140]

The use of cyberspace to carry out offensive action is not solely the domain of states, but also extends to non-state actors, chief among them terrorist networks. As a result, another major theme in the academic literature in terms of how cyberspace can impact international security is cyberterrorism. Although, like terrorism itself, there is a debate among scholars in defining cyberterrorism, Keiran Hardy and George Williams provide a legal definition covering the main aspects of the term:

> 'Cyberterrorism' means conduct involving computer or Internet technology that (1) is carried out for the purpose of advancing a political, religious or ideological cause; (2) is intended to intimidate a section of the public, or compel a government to do or abstain from doing any act; and (3) intentionally causes serious interference with an essential service, facility or system, if such interference is likely to endanger life or cause significant economic or environmental damage.[141]

---

[139] Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36.1 (2013): 101-08.

[140] Several studies highlight that only a handful of states have the technical resources to develop cyber weapons. For example, see: Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies* 35.5 (2012): 689-711.; Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22.3 (2013): 365-404.

[141] Hardy, Keiran, and George Williams. "What Is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism." *Cyberterrorism Understanding, Assessment, and Response.* Ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald. New York, NY: Springer, 2014. 1-23.

Gabriel Weimann identifies six factors that make cyber operations an attractive option for terrorist groups.[142] First, cyber operations require a minimal expenditure of resources when compared to conventional operations. Cyberspace allows for a far greater degree of anonymity than in the real world as well, allowing terrorists to better cover their tracks. It also enables terrorist groups to remotely attack areas that traditionally may have been outside of their geographical reach. Next, cyberspace presents a target rich environment in which terrorist networks can exploit a wide range of vulnerabilities. This in turn also allows a far greater scope of damage given that terrorists can target Critical Information Infrastructures (CIIs) of "telecommunications, power grids, transport and storage of gas and oil, banking and finance, traffic, water supply systems, emergency rescue services and public administration."[143] Finally, cyber terrorism has a greater fear factor because, unlike physical reality, individuals have lesser degree of control over the digital domain to protect themselves.

Although the potential of cyber terrorism seems profound, does it pose a threat in reality? Dorothy E. Denning has conducted comprehensive research on the following five categories of evidence to evaluate the capability or intent of terrorist networks to carry out cyber operations: 1) all cases of cyber attacks, including cyber-terrorism; 2) cyber weapons acquisition and distribution, research and development, and training; 3) statements about cyber attacks, including discussions, declarations of intent, and entreatment for others to conduct cyber attacks; 4) education in information technology, specifically in network and information security; and 5) general experience with cyberspace in the communication and dissemination of news and

---

[142] Weimann, Gabriel. *Terrorism in Cyberspace: The next Generation*. New York: Columbia University Press, 2015.

[143] Dunn Cavelty, Myriam. "Critical Information Infrastructure: Vulnerabilities, Threats and Responses." *UNIDIR Disarmament Forum*.3 (2007): 15-22.

propaganda. Denning's research on these categories of evidence concludes that: "The foregoing evidence shows that terrorist groups and jihadists have an interest in conducting cyber attacks and at least some capability to do so. Further, they are attempting to develop and deploy this capability through online training and calls for action. The evidence does not, however, support an imminent threat of cyberterrorism."[144]

This argument is echoed in Giampiero Giacomello's cost-benefit analysis of cyber terrorist operations, which highlights how traditional methods of terrorism in many instances are still more efficient than cyber operations for terrorist networks. At the same time, he acknowledges that cyberspace is "more effective for the terrorists to exploit information infrastructures to fight a "war of ideas," spreading their beliefs and points of view."[145] In the same vein, Maura Conway argues that we should consider cyber terrorism as only one risk among the spectrum of risks associated with the use of cyberspace by the terrorist networks, covering a broad range of activities including media operations, recruitment, learning, financing, and enhancing their communication and operational security.[146] The unprecedented use of cyberspace by the Islamic State to conduct a slick propaganda campaign to attract recruits, including self-radicalized "lone wolves",[147] intimidate enemies, energize sympathizers, and garner funds, validates this scholarly perspective.

---

[144] Denning, Dorothy E. "A View of Cyberterrorism Five Years Later." *Internet Security: Hacking, Counterhacking, and Society*, Ed. Kenneth Einar. Himma. Sudbury, MA: Jones and Bartlett Publishers, 2007. 123-40. p.135.

[145] Giacomello, Giampiero. "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism." *Studies in Conflict & Terrorism* 27.5 (2004): 387-408.

[146] Conway, Maura. "Terrorism and New Media: The Cyber-Battlespace." *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, Ed. James J. F. Forest, Vol. 2. Westport, CT: Praeger Security International, 2007. 363-84.

[147] Weimann, Gabriel. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3.2 (2012): 75-90.

1.4.2. Transformation of the Global Economy in the Information Age

Another major global impact of cyberspace is its transformation of the global economy. This is mainly because Information and Communication Technologies (ICTs), which constitute the crux of cyberspace, are the most advanced types of what scholars call General Purpose Technologies (GPTs). According to Erik Brynjolfsson and Adam Saunders the four following characteristics of GPTs make them a powerful engine of economic development: 1) the wide scope for improvement and elaboration; 2) applicability across a broad range of uses; 3) potential for use in a wide variety of products and processes; and 4) strong complementarities with existing or potential new technologies.[148]

Information and Communication Technologies are now considered among the most important determinants of economic growth. This is evident in the findings of several empirical studies on economic growth in the G7 countries, United States, United Kingdom, Spain, Finland, Greece, Japan, and Singapore, among others.[149] Among the most comprehensive case studies in the field is Khuong M. Vu's research on ICT as a source of economic growth. Analyzing data for 102 countries in the 10 years between 1996 and 2005, this research shows that ICT penetration had a robust causal link with the significant economic growth we have witnessed in this period as

[148] Brynjolfsson, Erik, and Adam Saunders. *Wired for Innovation: How Information Technology Is Reshaping the Economy*. Cambridge, MA: MIT Press, 2010. p.95.

[149] Jorgenson, Dale W. "Information Technology and the G7 Economies." *World Economics* 4.4 (2003): 139-69.; Jorgenson, Dale W. "Information Technology and the US Economy." *The American Economic Review* 91.1 (March 2001): 1-32.; Oulton, Nicholas. "ICT and Productivity Growth in the United Kingdom." *Oxford Review of Economic Policy* 18.3 (2002): 363-79.; Martínez, Diego, Jesús Rodríguez, and José L. Torres. "The Productivity Paradox and the New Economy: The Spanish Case." *Journal of Macroeconomics* 30.4 (2008): 1569-586.; Jalava, Jukka, and Matti Pohjola. "ICT as a Source of Output and Productivity Growth in Finland." *Telecommunications Policy* 31.8-9 (2007): 463-72.; Antonopoulos, Christos, and Plutarchos Sakellaris. "The Contribution of Information and Communication Technology Investments to Greek Economic Growth: An Analytical Growth Accounting Framework." *Information Economics and Policy* 21.3 (2009): 171-91.; Jorgenson, Dale, and Kazuyuki Motohashi. "Information Technology and the Japanese Economy." *Journal of the Japanese and International Economies* 19.4 (2005): 460-81.; Vu, Khuong M. "Information and Communication Technology (ICT) and Singapore's Economic Growth." *Information Economics and Policy* 25.4 (2013): 284-300.

compared to the previous two decades.[150] Vu points to three main channels through which ICT can make such a strong contribution to economic growth: 1) fostering technology diffusion and innovation; 2) enhancing the quality of decision-making by firms and households; and 3) increasing demand and reducing production costs, which together raises the output level.

Despite the general consensus in the literature about the positive role of ICT in economic development, scholars have highlighted that not everyone benefits from it evenly. Instead, what we are witnessing now is a "digital divide" both within and between societies.[151] According to the World Bank's World Development Report 2016:

> The lives of the majority of the world's people remain largely untouched by the digital revolution. Only around 15 percent can afford access to broadband internet. Mobile phones, reaching almost four-fifths of the world's people, provide the main form of internet access in developing countries. But even then, nearly 2 billion people do not own a mobile phone, and nearly 60 percent of the world's population has no access to the internet. The world's offline population is mainly in India and China, but more than 120 million people are still offline in North America.[152]

The report also highlights the state of digital divide within the countries:

> Worldwide, nearly 21 percent of households in the bottom 40 percent of their countries' income distribution don't have access to a mobile phone, and 71 percent don't have access to the internet. Adoption gaps between the bottom 40 percent and the top 60 percent and between rural and urban populations are falling for mobile phones but increasing for the internet.[153]

---

[150] Vu, Khuong M. "ICT as a Source of Economic Growth in the Information Age: Empirical Evidence from the 1996–2005 Period." *Telecommunications Policy* 35.4 (2011): 357-72.

[151] Norris, Pippa. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. New York: Cambridge University Press, 2001.

[152] WB. "World Development Report 2016: Digital Dividends." *The World Bank*. 2016. Web. 07 August 2016. <http://www.worldbank.org/en/publication/wdr2016>. p.6.

[153] Ibid. p.7.

Sanjeev Dewan and Frederick J. Riggins identify two major analytical approaches to the digital divide in the academic literature. The first approach defines the term mainly based on a dichotomy between the haves and have-nots when it comes to access to the Information and Communication Technologies.[154] This approach equates access and use of ICT, assuming that all people online have the same ability to use and benefit from these technologies. The second approach goes beyond this simple dichotomy, underlying various economic and social factors that cause the digital divide through their impact on the use of ICT, including income, race, gender, geography, culture, education, and technical skills. These factors are so significant that many scholars assert that the digital divide simply mirrors the socio-economic inequalities of the real world. Jan van Djik, a leading scholar on this subject, articulates a number of general factors which contribute to creating the digital divide, that effectively synthesize the above two approaches, including:

> The availability and cost of digital technology in a country; a country's general level of literacy and education; the language skills of a country's population, speaking English in particular; the level of democracy (freedom of expression); the strength of policies to promote the information society in general and access in particular; a culture that is attracted to technology, computers, and computer communication.[155]

The consequences of the digital divide are by no means trivial, but can result in wide-ranging social exclusion within and between societies, with devastating consequences for a state's development and relations with other states. The digital divide, according to Allen Hammond, could lead to security challenges by depriving certain segments of the population of the digital

---

[154] Dewan, Sanjeev, and Frederick J. Riggins. "The Digital Divide: Current and Future Research Directions." *Journal of the Association for Information Systems* 6.12 (2005): 298-337.

[155] Van Djik, Jan A. G. M. "One Europe, Digitally Devide." *Routledge Handbook of Internet Politics*, Ed. Andrew Chadwick and Philip N. Howard, 288-304. London: Routledge, 2009. 288-304. p.292.

revolution's benefits and pushing them to embrace violence to acquire their share.[156] Accordingly, many researchers conduct policy-oriented studies to tackle the issue of the digital divide. The first major policy approach postulates that market forces play the most significant role in bridging this divide. In this approach, governments need not interfere because subsidies or other such interventions can distort patterns of investment and result in the inefficient allocation of resources. A competitive environment, in contrast, is thought to encourage innovation and a decrease prices for users.[157] Consequently, Global South countries in particular are called upon to accelerate liberalization of the their telecommunication sectors to achieve these benefits.[158] This approach has been criticized for being overly market-centric, with a second approach emphasizing that in fact the digital divide will not diminish without governmental intervention.[159] It encourages government intervention on the grounds that it is necessary to create the right conditions for market development.[160] Although market competition is considered essential for the efficient allocation of services and technological innovation, there are sectors of society - low-income, rural, and low-density areas - that are likely to remain

---

[156] Hammond, Allen L. "Digitally Empowered Development." *Foreign Affairs* 80.2 (2001): 96-106.

[157] Guillen, Mauro F., and Sandra Suarez L. "Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use." *Social Forces* 84.2 (2005): 681-708.; Lai, Bruce, and Gale Brewer A. "New York City's Broadband Problem and the Role of Municipal Government in Promoting a Private-sector Solution." *Technology in Society* 28.1-2 (2006): 245-59.; Andrés, Luis, David Cuberes, Mame Diouf, and Tomás Serebrisky. "The Diffusion of the Internet: A Cross-country Analysis." *Telecommunications Policy* 34.5-6 (2010): 323-40.

[158] WB. "Information and Communications for Development: Global Trends and Policies." *The World Bank*. 2006. Web. 08 August 2016. <http://documents.worldbank.org/curated/en/692321468170348192/Overview>.

[159] Kudaisya, Gyanesh. "India's New Mantra: The Internet." *Current History* 100.645 (2001): 162-69.; Chowdary, T.h. "Diminishing the Digital Divide in India." *INFO* 4.6 (2002): 4-8.; Alden, Christopher. "Let Them Eat Cyberspace: Africa, the G8 and the Digital Divide." *Millennium - Journal of International Studies* 32.3 (2003): 457-76.; Bleha, Thomas. "Down to the Wire." *Foreign Affairs* 84.3 (2005): 111-17.; Mathur, Akshay, and Dhirubhai Ambani. "ICT and Rural Societies: Opportunities for Growth." *The International Information & Library Review* 37.4 (2005): 345-51.

[160] Cava-Ferreruela, Inmaculada, and Antonio Alabau-Muñoz. "Broadband Policy Assessment: A Cross-national Empirical Analysis." *Telecommunications Policy* 30.8-9 (2006): 445-63.

underserved, requiring government support. Therefore, this framework encourages governments to intervene in a number of ways, including by subsidizing internet access to underserved demographics, building ICT infrastructure, and creating facilities available for public use.

The academic literature reviewed above has highlighted the significance that cyberspace has had for the structure of the global economy and how states can exploit this huge potential to achieve their economic development goals. Chapter four engages in a detailed examination of the measures taken by the IRI to exploit this potential for its own development. There is a comparison of the impact of cyberspace on the Iranian economy versus those of a sample of economies in the Caucasus, Central Asia, and Middle East, drawing on four of the main global indexes for information and communication technology development.

1.4.3. Emergence of Global Cyber Governance

Exploring the political impact of cyberspace at the global level, we have discussed the security and economic dimensions. The desire of states to exert authority over cyberspace, when combined with the inherently international architecture and connections of this space, leads to another dimension: global cyber governance. At the heart of the elevation of cyberspace to an issue of global governance is a "strong and persistent tension between state sovereignty, which is territorially bounded, and the non-territorial space for social interaction created by networked computers."[161] According to Milton L. Mueller, cyberspace has parallels to trade and the environment as global issues which, due to their inherently transnational nature, have spawned whole global institutions of governance: "like global trade and environmental policy, Internet

[161] Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010. p.1.

governance has become a point of international conflict among states and a target of transnational policy advocates from business and civil society."[162]

A leading example of global institutions for cyber governance is the Internet Corporation for Assigned Names and Numbers (ICANN). An American private, not-for-profit, and multi-stakeholder organization founded in 1998, ICANN is overseen by an international board of directors given authority over the Internet through its power to manage internet protocol (IP) addresses and the domain name system (DNS).[163] IP addresses and the DNS system are designed to work together to allow humans straightforward access the Internet. While the computers that collectively constitute the Internet speak to one another through numbers linked to specific devices called IP addresses, in reality it is not practical for humans to try to remember long lists of these numbers. The DNS system, which uses letters instead of numbers, was designed to allow humans to link a precise series of letters with a precise series of numbers to make searching the Internet more straightforward. Therefore, DNS makes a link between "52.202.119.65", the University of Alberta website IP address, to the name "ualberta.ca", to name just one example.

Nation states often view the particular institutional set up of ICANN problematic along two main lines of argument: First, ICANN is based on a multi stakeholder model dominated by the private sector and non-governmental organizations (NGOs), diminishing the influence which states have to shape the policies and practices of this organization. Second, the physical presence of ICANN inside the jurisdiction of the United States creates the appearance and perhaps even reality of

---

[162] Ibid.

[163] Mathiason, John. "The ICANN Experiment." *Internet Governance: The New Frontier of Global Institutions.* London: Routledge, 2009. 70-96.

undue US influence over it. For example, in the American court case *Rubin et al v. Islamic Republic of Iran et al* the American victims of a suicide bombing by Hamas in Jerusalem were given an award against the Iranian government. This was done on the basis of the latter's alleged responsibility for the victims' deaths due to its material support for Hamas, and subsequently the plaintiffs tried to seize the '.ir' domain associated with Iran as part of their award. While ICANN resisted the seizure and was supported by a higher court, this attempt has created a precedent in which the United States and its citizens can utilize the physical presence of this organization on American territory to their advantage.[164]

The Internet Corporation for Assigned Names and Numbers' dual issues of multi-stakeholderism and presence in US jurisdiction have continually been raised and debated in different cyber governance forums. One of the forums in which these issues have been hashed out is the World Summit on the Information Society (WSIS), a United Nations sponsored series of conferences that discussed global ICT issues and incorporate dozens of state, private sector, and civil society representatives.[165] In the first phase of these conferences, held in Geneva in 2003, the countries critical of ICANN's set up raised the aforementioned two issues. They further formed a bloc promoting a state-centric model of governance "through elections and legislation at the national level and the multilateral negotiation of agreements among sovereign peers at the international level."[166] The net result of this phase was the Geneva Declaration of Principles, which enshrined

---

[164] Levinson, Nanette S., and Laura DeNardis. "Governance by Infrustructure." *The Turn to Infrastructure in Internet Governance.* Ed. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson. New York: Palgrave Macmillan, 2016. 3-21.

[165] Hubbard, Amanda, and Lee Bygrave A. "Internet Governance Goes Global." *Internet Governance: Infrastructure and Institutions*, Ed. Lee Bygrave A. and Jon Bing. Oxford: Oxford University Press, 2009. 213-35.

[166] Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010. p.64.

the state-centric governance model and divided the questions at stake into public policy and technical issues. The declaration placed public policy firmly into the hands of states, remarking that "Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues."[167] While the declaration still accorded what it called an "important role" to the private sector on a technical level and to civil society on a community level, the language regarding these roles remained vague and a clear hierarchy, in which states had the preeminent role, was established.

The Geneva Declaration of Principles also called on the UN secretary general to create a group, which became the Working Group on Internet Governance (WGIG), to develop a definition of Internet governance, study the policy issues that exist, and formulate the roles and responsibilities of different stakeholders. This process culminated in the 2005 report of the WGIG, which stated that "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet."[168] The WGIG report's emphasis on "respective roles" recalled the division of labor in the Geneva Declaration of Principles between states' prerogative on public policy versus the private sector's role in technical issues and civil society's role in community issues. The WGIG report thus continued the state-centric vision of this declaration in its work. The report also suggested a number of organizational models for global cyber governance, three of which

---

[167] ITU. "Declaration of Principles (Building the Information Society: A Global Challenge in the New Millennium)." *International Telecommunication Union (ITU)*. 12 December 2003. Web. 08 August 2016. <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>.

[168] De Bossey, Château. "Report of the Working Group on Internet Governance." *The Internet Governance Forum (IGF)*. June 2005. Web. 08 August 2016. <http://www.wgig.org/docs/WGIGREPORT.pdf>.

recommended replacing ICANN with a new international body that was more inclusive in terms of the diversity of actors. The fourth model called for preserving ICANN while recommending a set of adjustments in the structure of the organization.

The second phase of the WSIS conference series unfolded in Tunis in 2005. During this phase the main debates broke down along the lines of two familiar questions. The first was whether cyber governance would emphasize multi-stakeholderism, meaning that it would include participation from states, the private sector, and civil society, versus multilateralism, which prioritized discussion and cooperation among states. The second question revolved around the future role of ICANN given the appearance of undue American influence over it. The outcome of this phase was the Tunis Agenda for the Information Society.[169] This text ultimately adopted the fourth model proposed by WGIG for ICANN highlighted above in which the latter would continue to have a role but incorporate changes that, among other things, reduced its American-centrism. However, it nonetheless continued to prioritize states, meaning the issue of multi-stakeholderism versus multilateralism was left unresolved. In particular, the agenda called for the creation of an Internet Governance Forum (IGF) which would meet annually around the world and promote further dialogue on these two issues. In its subsequent IGF meetings, the debate over multi-stakeholderism versus multilateralism continued to dominate, while the discussion over ICANN itself became of secondary significance.

This debate has subsequently played out in other forums, one of the most prominent and contentious episodes being the World Conference on International Telecommunications

---

[169] ITU. "Tunis Agenda for the Information Society." *International Telecommunication Union (ITU)*. 18 November 2005. Web. 08 August 2016. <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

(WCIT-12) hosted by the United Nations' International Telecommunication Union (ITU) in Dubai in 2012. The conference sought to revise the International Telecommunication Regulations (ITRs) of 1988 to bring it into line with the profound technological changes witnessed in the 21st century. Resolution 03 of the proposed final text of the ITRs, entitled "To foster an enabling environment for the greater growth of the Internet", became emblematic of the division created by the multi-stakeholderism versus multilateralism debate.[170] Critics of the resolution argued that the role of states continued to be overemphasized at the expense of other stakeholders and that states were actually gaining new rights in this process that threatened both individual rights and economic growth. This profound division was reflected in the conference's failure to gain consensus over revision of the ITRs, with 89 signing to bring these changes into effect but 55 refusing to do so.

The question over the role of ICANN was finally put to rest shortly following the 2014 NETmundial Conference in Sao Paulo. The conference, unlike the ITU one in Dubai in 2012 which focused almost exclusively on states, brought together more than 900 participants from governments, civil society, and the private sector, to continue the key debates over the future of cyber governance. The non-binding resolution of this conference, unlike WCIT-12, promoted multi-stakeholderism over multilateralism.[171] This resolution was supported by a majority bloc that included the United States, Canada, and Australia, who favored this model, and opposed by a minority bloc that included countries like Russia, China, and India, which refused to sign given

---

[170] ITU. "Final Acts of the World Conference on International Telecommunications (WCIT-12)." *The International Telecommunication Union (ITU)*. 2012. Web. 10 Dec. 2016. <https://www.itu.int/pub/S-CONF-WCIT-2012/en>.

[171] NM. "NETmundial Multistakeholder Statement." *NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance*., 24 Apr. 2014. Web. 10 Dec. 2016. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

their preference for cyber governance as an issue best dealt with between governments and within the United Nations framework. A month following this conference in March 2014 the United States pledged to turn ICANN over to a global multi-stakeholder community, effectively putting an end to question over the role of ICANN and America's influence over it.[172] This means that global cyber governance debates are likely to be dominated by the multi-stakeholder versus multilateral debate, at least for the foreseeable future. The genealogy and trajectory of these debates is discussed at length in chapter five. We then look at how the IRI has positioned itself in these debates and pursued its interests through the emerging institutions of global Internet governance.

1.4.4. Public Diplomacy in the Global Information Age

The last section of this literature review on the impact of cyberspace on global politics deals with Public Diplomacy, or advancing foreign policy objectives by engaging with foreign publics. Conducting a comprehensive review of the academic literature on diplomacy definitions, Benno H. Signitzer and Timothy Coombs distinguish between diplomacy and public diplomacy underlining that diplomacy has been traditionally understood as the "art of conducting negotiations between governments", whereas public diplomacy is "the way in which both government and private individuals and groups influence directly or indirectly those public attitudes and opinions which bear directly on another government's foreign policy decisions".[173]

---

[172] NITA. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." *National Telecommunications and Information Administration.* United States Department of Commerce, 14 Mar. 2014. Web. 10 Dec. 2016. <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

[173] Signitzer, Benno H., and Timothy Coombs. "Public Relations and Public Diplomacy: Conceptual Convergences." *Public Relations Review* 18.2 (1992): 137-47. p.138.

In the same vein, Gifford D. Malone argues that the core idea of public diplomacy is the "direct communication with foreign peoples, with the aim of affecting their thinking and, ultimately, that of their governments."[174] Howard H. Frederick asserts that public diplomacy incorporates "activities, directed abroad in the fields of information, education, and culture, whose objective is to influence a foreign government, by influencing its citizens."[175]

The transmission of information through communication channels between governments and foreign publics constitute the main pillars of public diplomacy. Accordingly, the emergence of ICTs has significantly transformed public diplomacy in terms of both the quality and extent of engagement of governments with foreign publics.[176] Jan Melissen highlights that communication with foreign publics en masse and moving from one-way information flow towards two-way exchange and engagement are among the most significant characteristics of the "new public diplomacy" in information era. He emphasizes that "the new public diplomacy is no longer confined to messaging, promotion campaigns, or even direct governmental contacts with foreign publics serving foreign policy purposes. It is also about building relationships with civil society actors in other countries and about facilitating networks between non-governmental parties at home and abroad."[177]

---

[174] Malone, Gifford D. "Managing Public Diplomacy." *The Washington Quarterly* 8.3 (1985): 199-213. p.199.

[175] Frederick, Howard H. *Global Communication & International Relations*. Belmont, CA: Wadsworth, 1993. p.229.

[176] Kurbalija, Jovan. "Diplomacy in the Age of Information Technology." *Innovation in Diplomatic Practice*, Ed. Jan Melissen. New York: St. Martin's Press, 1999. 171-91; Kurbalija, Jovan. "The Impact of the Internet and ICT on Contemporary Diplomacy." *Diplomacy in a Globalizing World: Theories and Practices*, Ed. Pauline Kerr and Geoffrey Wiseman. New York: Oxford University Press, USA, 2013. 141-59.

[177] Melissen, Jan. "The New Public Diplomacy: Between Theory and Practice." In *The New Public Diplomacy: Soft Power in International Relations*, by Jan Melissen, 3-26. Basingstoke: Palgrave Macmillan, 2005. p.22.

Nicholas Cull presents a useful taxonomy of five core components of public diplomacy and shows how the use of cyberspace has enhanced all these components.[178] The first component is "Listening", which consists of collecting and collating data about foreign publics' opinion and using that data to design and evaluate the effect of public diplomacy conduct on targeted publics. The second component is "Advocacy", or active engagement with foreign public to promote a particular policy or idea in the minds of targeted publics through an outward flow of information. The third component is "Cultural Diplomacy", making cultural resources and achievements known abroad or simply facilitating the export of examples of culture. Next is "Exchange Diplomacy", or sending citizens abroad and reciprocally accepting foreign citizens for a period of study and/or acculturation. The fifth and final component is "international news broadcasting", or engaging with foreign publics en masse mainly through the circulation of news among them. Cull deftly weaves together the way in which the communication power embedded in cyberspace has been transformative for each of the five core components of public diplomacy, characterizing public diplomacy in the information era as such:

> It is a form of listening in as much as it provides a mechanism for views from the public to be transmitted back to the actor in the form of comments, tweets, likes, and the highly revealing path of re-tweets, re-postings, and tracking of particular phrases or ideas across the blogosphere. It is a form of advocacy in as much as its channels can be used to present the actor's point of view. It is a form of cultural diplomacy in both the sense of transmitting culture through content and being a culture in its own right. It is a form of international broadcasting in as much as it facilitates the circulation of news across frontiers and has provided a new platform for the traditional international broadcasters. Perhaps its greatest potential and closest fit is as a form of exchange diplomacy, which like the social media seeks to operate through networks and people-to-people connections. Here then was the perfect medium for the new public diplomacy.[179]

---

[178] Cull, Nicholas J. "The Long Road to Public Diplomacy 2.0: The Internet in US Public Diplomacy." *International Studies Review* 15.1 (2013): 123-39.

[179] Ibid. p.125.

At the heart of Cull's concept of public diplomacy is the notion of one state overtly attempting to persuade the public of another state in accordance with its own agenda and interests. The recent experience of alleged Russian interference in the 2016 U.S. presidential election underscores a possibility not contemplated by this conceptualization of public diplomacy, but which uses many of the same elements of cyberspace.[180] In the 2016 election, Russia attempted to use leaks of hacked data online and social media tools to create a negative impression of Democratic Party candidate Hillary Clinton in the minds of the American public and persuade them to vote for Republican Party candidate Donald Trump. Although this effort has similarities to public diplomacy, in that it targeted the public of a rival state to achieve a desired political outcome, it had at least two distinguishing features: The Russians attempted to turn the public of another state against their own government, rather than in favor of themselves, and they were covert. At present the literature is silent on this type of cyber action and further research is required to go beyond this anecdote to a more explanatory conceptual framework.

The academic literature on public diplomacy in the cyber era, often called digital public diplomacy, is mainly focused on the United States which was among the first and most prolific countries to realize the potential use of cyberspace for conducting public diplomacy in the early 2000's. Recognizing the changes in the international relations and conditions of "statecraft in the 21st century", the US government was quick to call for transformation of US foreign policy institutions in order to complement "traditional foreign policy tools with newly innovated and adapted instruments of statecraft that fully leverage the technologies of our interconnected

[180] Walker, Christopher, and Jessica Ludwig. "The Meaning of Sharp Power." *Foreign Affairs*, 16 Nov. 2017. Web. 07 Apr. 2018. <https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power>.; Nye, Joseph S. "How Sharp Power Threatens Soft Power." *Foreign Affairs*. 24 Jan. 2018. Web. 07 Apr. 2018. <http://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power>.

world".[181] This is in part manifested in the 230 Facebook pages, 80 Twitter accounts, 55 channels on YouTube, and 40 Flickr pages operated by the State Department as of 2010, with the commitment of the department to utilize cyberspace only increasing over time.[182]

The body of literature on US digital public diplomacy covers different sets of topics including: the history of US digital public diplomacy;[183] US digital public diplomacy to counter the narrative of terrorist groups like Al-Qaeda and crafting a credible counter-narrative;[184] use of blogging and micro-blogging platforms in US digital public diplomacy,[185] and US cyber public diplomacy initiatives such as the State Department's Digital Outreach Team (DOT).[186] The DOT is a small team of State Department officials who engage in discussions in different languages, including Arabic, Farsi and Urdu, on several social media platforms and internet discussion forums in order to "explain US foreign policy and to counter misinformation".[187] DOT members identify themselves by name and acknowledge that they are affiliated with the State Department.

The US conduct of cyber public diplomacy toward Iran is particularly interesting given the lack of formal relations between the countries and the obstacles for the United States to gaining direct

---

[181] USDS. "21st Century Statecraft." *U.S. Department of State*. 2009. Web. 11 August 2016. <http://www.state.gov/statecraft/overview/index.htm>.

[182] Seib, Philip M. *Real-time Diplomacy: Politics and Power in the Social Media Era*. New York: Palgrave Macmillan, 2012. p.169.

[183] Hanson, Fergus. "Baked In and Wired: EDiplomacy@State." *Brookings*. 25 October 2012. Web. 08 August 2016. <https://www.brookings.edu/wp-content/uploads/2016/06/baked-in-hansonf-5.pdf>.

[184] Hallams, Ellen. "Digital Diplomacy: The Internet, the Battle for Ideas & US Foreign Policy." *CEU Political Science Journal* 5.4, 538-74.

[185] Zhong, Xin, and Jiayi Lu. "Public Diplomacy Meets Social Media: A Study of the U.S. Embassy's Blogs and Micro-blogs." *Public Relations Review* 39.5 (2013): 542-48.

[186] Khatib, Lina, William Dutton, and Michael Thelwall. "Public Diplomacy 2.0: A Case Study of the US Digital Outreach Team." *The Middle East Journal* 66.3 (2012): 453-72.

[187] Seib, Philip M. *Real-time Diplomacy: Politics and Power in the Social Media Era*. New York: Palgrave Macmillan, 2012. p.121.

access to the Iranian public. In 2011, the State Department launched a website called Virtual Embassy in Iran, the first of its kind, to provide "the primary official resource for the Iranian people to get information directly from the US government about US policy and American values and culture."[188] With the absence of an embassy presence and formal diplomatic relation for three decades since the hostage crisis of 1979, the virtual embassy now plays an important role in the US cyber public diplomacy toward the Iranian public. Furthermore, the State Department now manages USAdarFarsi pages on different social platforms including Facebook, Twitter, YouTube, Google+, Instagram and Telegram to engage with Iranian public.[189] Although the US is the main focus of the academic literature, there are several case studies about cyber public diplomacy in other countries, including: India, Sweden, Norway, Canada and the Netherlands.[190] There are also number of comparative studies on the conduct of digital diplomacy in different countries, including: the UK and Canada, US and Australia, US and Venezuela, South Korea and Japan, and cyber public diplomacy of the EU, US and Japan

---

[188] VEUS. "Why Virtual Embassy?" *Virtual Embassy of the United States - Tehran, Iran*. Web. 07 Apr. 2018. <https://ir.usembassy.gov/tehran/>.

[189] Maloney, Suzanne. "Iran: Public Diplomacy in Vacuum." *Isolate or Engage: Adversarial States, US Foreign Policy, and Public Diplomacy*, Ed. Geoffrey Wiseman. Palo Alto: Stanford University Press, 2015. 164-204. p.183.

[190] Natarajan, Kalathmika. "Digital Public Diplomacy and a Strategic Narrative for India." *Strategic Analysis* 38.1 (2014): 91-106.; Pelling, Jon. "When Doing Becomes the Message: The Case of the Swedish Digital Diplomacy." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 164-80.; Bátora, Jozef, and Iver Neumann B. "Cautious Surfers: The Norwegian Ministry of Foreign Affairs Negotiates the Wave of the Information Age." *Diplomacy & Statecraft* 13.3 (2002): 23-56.; Copeland, Daryl. "Virtuality, Diplomacy, and the Foreign Ministry: Does Foreign Affairs and International Trade Canada Need a "V Tower"?" *Canadian Foreign Policy Journal* 15.2 (2009): 1-15.; Van Noort, Carolijn. *Social Media Strategy: Bringing Public Diplomacy 2.0 to the next Level*. San Francisco: Consulate General of the Netherlands, 2011.; Bjola, Corneliu, and Lu Jiang. "Social Media and Public Diplomacy: A Comparative Analysis of the Digital Diplomatic Strategies of the EU, U.S. and Japan in China." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 71-88.

towards China.[191] In recent years Iran has also taken cyberspace as a tool in its public diplomacy arsenal, with the social media accounts of the supreme leader, president, and foreign minister (especially on Twitter and Instagram), among others, becoming important instruments for direct engagement with foreign publics. A desire and will clearly exists on the part of Iran to further utilize cyber public diplomacy. However, the IRI has not engaged in an organized and systematic public diplomacy campaign in relation to the publics of foreign states. At the same time, the IRI has recognized the significance and effectiveness of public diplomacy of foreign states, particularly adversaries in the West, in terms of influencing the Iranian public. The response of the IRI has primarily been to employ coercive measures, discussed at length in chapter three, and to bolster its own efforts to promote its political ideals, cultural values, policies and achievements in cyberspace, explored in chapter six.

Conclusion

Cyberspace has significant implications for state-society and international relations that leads states to endeavor to manage it as an emerging domain of power. Through a comprehensive review of the academic literature, this chapter examined and clustered these implications around eight major themes. Four of these themes revolve around state-society relations, including: social mobilization; collective action repertoires; generating and framing media coverage; and state propaganda, surveillance, and denial of access. The other four themes are centered on

---

[191] Clarke, Amanda. "Business as Usual? An Evaluation of British and Canadian Digital Diplomacy as Policy Change." In *Digital Diplomacy: Theory and Practice*, edited by Corneliu Bjola and Marcus Holmes, 111-27. New York: Routledge, 2015.; Murray, Stuart. "Evolution, Not Revolution: The Digital Divide in American and Australian Contexts." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 127-44.; Hayden, Craig. "Engaging Technologies: A Comparative Study of U.S. and Venezuelan Strategies of Influence and Public Diplomacy." *International Journal of Communication* 7 (2013): 1-25.; Park, Se Jung, and Yon Lim Soo. "Information Networks and Social Media Use in Public Diplomacy: A Comparative Analysis of South Korea and Japan." *Asian Journal of Communication* 24.1 (2014): 79-98.

international relations, including: international security; global economy; global cyber governance; and public diplomacy. The chapter also highlighted that the implications of cyberspace for state-society and international relations can be different, depending on the specific case, with context being just as important as the main characteristics of cyberspace itself in determining what outcomes will play out in a particular state.

With this in mind, it is easy to see how case studies can be essential for understanding the implications of cyberspace in a specific context. The case study as a research tool enables us to gain an in-depth understanding of a particular phenomenon, with certain observations being generalizable to cyberspace as a whole, while others will be unique to the specific case in question. While case studies on the implications of cyberspace on the domestic politics and foreign policy of specific states do exist, at present there is a dearth in terms of the number of states that have been closely observed. China is a good example of a state about which there are a number of case studies on this specific question, including Michael Chase and James Mulvenon's *You've Got Dissent!,* Zixue Tai's *The Internet in China*, Guobin Yang's *The Power of the Internet in China*, David Kurt. Herold and Peter Marolt's *Online Society in China*, and most recently Esarey and Kluver's *The Internet in China*.[192]

In the case of the Islamic Republic of Iran, however, no comprehensive case study looking at the IRI's cyber measures and their interaction with Iranian state-society and international relations

[192] See: Chase, Michael, and James Mulvenon C. *You've Got Dissent!: Chinese Dissident Use of the Internet and Beijing's Counter-strategies*. Santa Monica, CA: RAND, 2002.; Tai, Zixue. *The Internet in China: Cyberspace and Civil Society*. New York: Routledge, 2006.; Yang, Guobin. *The Power of the Internet in China*: *Citizen Activism Online*. New York: Columbia University Press, 2009.; Herold, David Kurt., and Peter Marolt, eds. *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*. Abingdon, Oxon: Routledge, 2011.; Esarey, Ashley, and Randy Kluver, eds. *The Internet in China: Cultural, Political, and Social Dimensions*. Great Barrington, MA: Berkshire Publishing Group, 2014.

exists. The review of the literature on Iranian cyberspace in this chapter has revealed that the majority of these works focus on how Iranian society has used cyberspace to pursue its own goals and interests. This means that the measures taken by the Iranian state to manage cyberspace have, by and large, remained understudied. The major exception to this trend in the literature is the IRI's comprehensive regime of filtering, which has been previously studied to some extent. The yet to be explored measures taken by the IRI include: the National Information Network (NIN); the restrictive body of law and the organizations that enforce it; defensive and offensive measures the IRI takes to establish deterrence against its adversaries at the global level; the state of the Iranian cyber economy and ICT development; the IRI's global Internet governance agenda ; and, lastly, the IRI's utilization of cyberspace for the propagation of its ideational factors associated with political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. The present doctoral project seeks to deepen the level of insight on the previously investigated aspects and establish a baseline for aspects yet to be examined, all within a coherent theoretical framework. It is therefore the intention of this project to fill a gap in the scholarly literature by asking the question: *what measures has the IRI adopted to manage the risks and opportunities of cyberspace as an emerging domain of power, and how have these measures interacted with Iranian state-society and international relations?*

CHAPTER TWO: THEORETICAL FRAMEWORK AND METHODOLOGY

Introduction

The introductory and literature review chapters of this dissertation have demonstrated that cyberspace is an emerging domain of power alongside well-established domains such as land, sea, air, and - more recently - space. Like these domains, cyberspace can be seen as an arena in which a range of political actors exercise power against one another, affecting state-society and international relations. As such, we cannot engage in a meaningful case study of the exercise of power in cyberspace without first arriving at a conceptualization of power. While individual aspects of the exercise of power in cyberspace have been addressed by previous works,[193] there is as of yet no comprehensive conceptualization that examines this subject in its multidimensional complexity for at least two reasons. First, the study of cyberspace as a domain of power is relatively new, in part because of the relative newness of the technology itself and its adaptation by political actors to apply power. Novel cases of the use of cyberspace to exercise power emerge with frequency and theoretical conceptualizations have struggled to grapple with the nuances of its unique dynamics. Second, the sheer quantity of actors and interactions embedded in cyberspace have revealed the inadequacies of our existing tools and methods for understanding the exercise of power in this new domain. When combined, these two factors have meant the realization of a conceptualization of power in cyberspace is, at least for the time being,

---

[193] Jordan, Tim. *Cyberpower: An Introduction to the Politics of Cyberspace*. London: Taylor and Francis, 2002; Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, D.C: Center for Technology and National Security Policy, 2009; Starr, Stuart H. "Towards an Evolving Theory of Cyberpower." *The Virtual Battlefield: Perspectives on Cyber Warfare*. Ed. Christian Czosseck and Kenneth Geers. Washington, DC: IOS, 2009. 18-52; Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. New York: Routledge, 2000; Hollon, Cory S. "New Domain, New Direction: Toward a Theory on Cyberspace Control and Use." *Defense Technical Information Center (DTIC)*, 1 Apr. 2012. Web. 01 Mar. 2018.<http://www.dtic.mil/docs/citations/AD1022966>.

a tall order. One approach to resolving this impasse is to undertake to devise an entirely new conceptualization of power for cyberspace. For reasons that should be evident, including that a single-case study can rarely aspire to lay the foundation for theory-building, however, such an endeavor is beyond the scope of this dissertation. A second, more practical, approach is to draw on existing conceptualizations of power to create a framework that is both compatible with cyberspace and addresses its multiple dimensions in a comprehensive manner. This dissertation has elected to take this second approach which will be discussed in detail below.

This chapter begins with the criticism of the materialist and state-centric conceptualization of power in structural realism, showing that in order to understand how power is exercised in cyberspace, we need a synthetic concept of power which highlights the significance of ideational factors and non-state actors in politics. Just as grappling with the exercise of power in cyberspace requires a multifaceted conceptualization of power, studying the political implications of cyberspace requires articulating a multifaceted methodological tool set. Once a conceptualization of power has been established, this chapter introduces the research design, rationale behind the single case study method used in this dissertation, and a set of methods for collecting quantitative and qualitative data, including: online public documents, the academic literature on cyberpolitics, semi-structured interviews, raw technical and macro-economic data, and social media data.

2.1 Conceptualization of Power

Power is a foundational concept in political science and the study of power relations is one of the most important functions of the discipline. Despite its foundational nature, power remains hotly contested in the discipline, and in the long history of political science there have been a number

of important debates around this concept.[194] A classic definition of power comes to us from Max Weber, who views *Macht* (power) as the ability of one actor in a social relationship to "carry out his own will despite resistance".[195] A more contemporary definition has been articulated by Robert A. Dahl. According to him: "A has power over B to the extent that he can get B to do something that B would not otherwise do".[196] These definitions, however, have been interpreted by subsequent scholars so as to center on coercion in one way or another. While coercion is a primary and self-evident dimension of power, it cannot be said to be all encompassing. There are contexts in which coercion is only one facet of power and is not fully explanatory. Cyberspace as a domain of power is precisely one such context.

International Relations as a discipline is taken as the starting point for synthesizing a conceptualization of power suitable for our analysis. This is in part because of the inherently global nature of cyberspace, in which territorial boundaries are no barrier to the ability of actors to influence one another. This section begins with the conceptualization of power in structural realism and argues while this may be a good starting point, it is not sufficient for examining how power is exercised in cyberspace. In order to suggest a more inclusive conceptualization of power, this chapter draws on the work of Robert W. Cox and Joseph S. Nye. This is because these conceptualizations highlight the role of non-state actors and ideational factors in global politics. The versatility of these conceptualizations allows us to account not only for the

---

[194] Bell, Roderick, ed. *Political Power: A Reader in Theory and Research*. New York: Free Press, 1969.

[195] Weber, Max. *The Theory of Social and Economic Organization*. New York, NY: Oxford University Press, 1947. p. 152. See also: Wallimann, Isidor, Nicholas Ch. Tatsis, and George V. Zito. "On Max Weber's Definition of Power." *Journal of Sociology* 13.1 (1977): 231-35.

[196] Dahl, Robert A. "The Concept of Power." *Behavioral Science* 2.3 (1957): 201-15. pp.202-3

implications of cyberspace for international relations, but also for state-society relations.[197] The following sections discuss the four major dimensions of power according to the conceptualizations of Cox and Nye. These are coercive power, economic power, power embedded in international institutions, and co-optive power generated from ideational sources, each explored in terms of how they are exercised in Iranian cyberspace in chapters three through six.

2.1.1. Coercive Power

Power has been one of the most integral concepts in discussions of international politics since Thucydides' analysis of the Peloponnesian War (431–404 BC). His observation that "the growth of the power of Athens, and the alarm which this inspired in Lacedaemon, made war inevitable," is seen as an early explanation of the behavior of states through power politics.[198] Although in the long tradition of international-political studies, the understanding of the nature of power has been contested among the scholars of the field, today this concept is largely formulated within the theoretical framework of structural realism.

According to Kenneth Waltz, a founding father of structural realism, there is no central authority overseeing international interactions and as a result the ordering principle of the international system is anarchy. As such, states, as the units of the international system, are forced to rely on themselves in order to guarantee their survival. In a system which is anarchic and requires self-help, the argument goes, it is logical for states to be as powerful as possible in order to counter

---

[197] The theoretical frameworks of Cox and Nye go beyond national/international dichotomy and analyses the linkages between state-society relations at the domestic level and international relations at the global level. In the same vein, James N. Rosenau presents a detailed analysis of complex interactions between domestic politics and global affairs. See: Rosenau, James N. *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World*. New York, NY: Cambridge University Press, 1997.

[198] Thucydides. *History of the Peloponnesian War*. Trans. Richard Crawley. Mineola, NY: Dover Publication, 2017. p.11.

the power of potentially hostile rival states. International politics, according to this framework, is mainly seen in terms of sovereign states aiming to preserve their security with what Alexander Wendt called "brute material forces"[199] as their ultimate instrument.[200] The centrality of materialism in Waltz's theory becomes clear when he defines state power as being based on: "size of population and territory, resource endowment, economic capability, military strength, political stability and competence".[201] Waltz then highlights that the major task for states in order to survive the anarchic international system is to transfer the aforementioned material sources of power into the first and constant *ultima ratio* in international politics, coercive force:

> The web of social and political life is spun out of inclinations and incentives, deterrent threats and punishments. Eliminate the latter two, and the ordering of society depends entirely on the former - a utopian thought impractical this side of Eden. Depend on threat and punishment, and the ordering of society is based on pure coercion. The daily presence of force and recurrent reliance on it mark the affairs of nations. Since Thucydides in Greece and Kautilya in India, the use of force and the possibility of controlling it have been the preoccupations of international-political studies.[202]

This conceptualization captures the first dimension of power for our discussion. Coercion can indeed explain key features of power dynamics in cyberspace. This includes the behavior of

---

[199] Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999. p.41.

[200] It must be emphasized that in the realist camp, it is mainly structural realism that in search for parsimony has formulated this materialist understanding of power. Classical realists like Hans Morgenthau and E. H. Carr did not share the same view of power. According to Morgenthau: "Power may comprise anything that establishes and maintains the control of man over man. Thus power covers all social relationships which serve that end, from physical violence to the most subtle psychological ties by which one mind controls another". In the same vein E. H. Carr divided the concept of power in the international sphere into three categories of military power, economic power, and power over opinion, emphasizing that the latter is "not less essential for political purposes than military and economic power, and has always been closely associated with them. The art of persuasion has always been a necessary part of the equipment of a political leader. Rhetoric has a long and honoured record in the annals of statesmanship". See: Morgenthau, Hans J. *Politics among Nations; the Struggle for Power and Peace*. New York: Knopf, 1985. p.11, and Carr, Edward Hallett. *The Twenty Years' Crisis, 1919-1939: An Introduction to the Study of International Relations*. London: Macmillan, 1946. p.132.

[201] Waltz, Kenneth Neal. *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979. p.131.

[202] Ibid. p.186.

states to take defensive measures to secure critical infrastructure against hostile cyber attacks. This also includes offensive measures by states to impose their will on adversaries and/or establish deterrence against them. Deterrence is the act of discouraging attack by an adversary by demonstrating one`s willingness and capability to respond in kind. Some doubt has been cast in the academic literature about the ability of states to deter if the very attribution of a cyber attack cannot be determined. As we saw in the literature review, anonymity is one of the key characteristics of cyberspace. The inability of a state to confirm the identity of an attacker raises question about just whom is sending a deterrence signal and against whom to retaliate. However, recent advances in technology that allow for better attribution have made the problem of attribution appear less serious than previously believed, and thus lends greater credence to the idea that deterrence through offensive capabilities is feasible. These dynamics in the context of Iranian cyberspace will be discussed at length in chapter three. The chapter will particularly examine the IRI's defensive measures to secure Iranian cyberspace against attacks by rival states, and the offensive measures adopted by the IRI to demonstrate its capability to retaliate against its rivals and establish deterrence.

Both Cox and Nye recognize the importance of coercion as a key dimension of power. Cox emphasizes that "material capabilities" are among the main sources for actors in global politics to exercise power. Part of these capabilities are what he calls "destructive capabilities" that lay at the heart of coercive power.[203] The "new realist" theoretical framework of Cox acknowledges the importance of coercion while also pointing out its inadequacies in terms of delineating other

[203] Cox, Robert W. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millennium: Journal of International Studies* 10.2 (1981): 126-55.

dimensions of power and non-state actors.[204] Nye also underscores that in the twenty-first-century coercive power is still the most important form of power on some domains or some issues.[205] However, he also points out that in a power-diffuse, economically interdependent, and culturally interconnected world, states are not the only important actors in global politics, security is not their only important concern, and coercive force emerging from material sources of power is not the only important instrument at their disposal.[206] As we will see in the following sections Cox and Nye criticize the short-sightedness of structural realism which views the existing global order ahistorically, thus being blind to how this order has changed over the course of history. They highlight the increasing trend of broad set of complex transnational connections and economic interdependencies between states and societies, emphasizing that such trends impose severe changes on global politics, including decreasing use of coercive force and giving rise to the significance of non-state actors, such as international institutions.[207] In this sense,

---

[204] Cox, Robert W., ed. *The New Realism: Perspectives on Multilateralism and World Order*. New York, NY: United Nations University Press, 1997.

[205] Nye, Joseph S. *The Future of Power*. New York, NY: PublicAffairs, 2011. p.28.

[206] Ibid. p.19.

[207] Another major line of criticism against structural realism came from post-structuralism which arose from the mid-1980s onward on the basis of important meta-theoretical questions and ethical issues. At the level of meta-theory post-structuralists mainly highlight the role of the knowledge-power relation in the production and understanding of structural realism as a dominant theoretical framework in the International Relations discipline. Drawing on Michel Foucault's conceptualization of power-knowledge, post-structuralists highlight how systems of power relations in any particular era determine what counts as true and which body of thought should be recognized as knowledge. In this regard, post-structuralists claim that ideas which are considered as self-evidently true are in fact the product of the power relations. Rather than produce a more accurate truth, then, the researcher should focus on bringing the operation of power to light and show how the will to power masquerades itself as the will to truth. In this sense, post-structuralists tried to illustrate how structural realism became not only dominant, but widely seen as 'common sense' and representing reality as such, meaning that all critiques came to be evaluated in light of it. Beyond strictly theoretical issues, post-structuralists were also unsatisfied with how structural realism had maintained its dominance despite the many obvious changes in the global political order, and thus embarked on the ethical project of incorporating perspectives, issues, and voices that structural realism had marginalized or excluded altogether. We shall not dwell on every aspect of the post-structural criticism against structural realism as that would go far beyond the scope of this dissertation. For more see: Campbell, David. "Poststructuralism." *International Relations Theories: Discipline and Diversity*. Ed. Tim Dunne, Milja Kurki, and Steve Smith. Oxford: Oxford University Press, 2013. 213-37; Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Trans. Alan Sheridan. New York, NY: Vintage, 1977; Foucault, Michel. *The Archaeology of Knowledge*. Trans. A. M. Sheridan Smith. London: Tavistock Publishers, 1972.

these thinkers see coercive power not as the *ultima ratio* in politics, but as one constitutive element of power along with economic power and the power embedded in political institutions. They also expand the conceptualization of power to go beyond *coercion*, which comes from material forces and demands obedience, and include *persuasion* which emerges out of ideational sources and encourages consent.

The conceptualization of coercive power, conceived in the context of global politics, can also be applied to the case of state-society relations at the domestic level. In fact, as Max Weber aptly highlighted, what defines the state in the first place is its "monopoly on the legitimate use of physical force" in the coercive enforcement of order within its territory.[208] The police, judiciary, penal code and mechanisms of punishment, among others, are just some of the instruments through which the state exercises coercion over society at the domestic level. In the context of cyberspace, the main pillars enabling a state to exercise coercive power at the domestic level include: a national intranet network which can territorialize cyberspace and wall it off from the global Internet; a comprehensive regime of filtering to limit the society's access to information; and a restrictive body of law regulating cyberspace in order to deter users from activities the state deems undesirable. Chapter three will examine the exercise of coercive power through these pillars in Iranian cyberspace.

2.1.2. Economic Power

As highlighted above, Cox and Nye do not limit their conceptualizations of power to coercion alone, but also emphasize the economic dimension of power. Both note that the foundation of

---

[208] Weber, Max. "Politics as a Vocation." *From Max Weber: Essays in Sociology*. Ed. Hans Gerth and C. Wright Mills. Abingdon, Oxon: Routledge, 1991. 77-128.

coercive power is economic power, in that it is a prosperous economy that provides the means to build the instruments of coercive power, particularly in the contemporary world where such power is very expensive at both the domestic and international levels. As already noted, Cox highlights that material capabilities are major resources of state power. One pillar of these material capabilities are "destructive capabilities", which generate the coercive power of the state. Another pillar of state's material capabilities is what he calls "productive capabilities", or the organizational and technological capacity of society and natural resources that produce wealth. Cox further points out, "Production creates the material basis for all forms of social existence, and the ways in which human efforts are combined in productive processes affect all other aspects of social life, including the polity."[209] Cox concludes that, "production relations can be a common yardstick, to which the other levels of power can be reduced".[210] Concurring with Cox, Nye argues that while coercion has been called "the ultimate form of power" in politics," a "thriving economy is necessary to produce such power".[211]

Economic power is also one of the foundations of the power embedded in international institutions, which allow a state to exercise power over actors by framing the agendas of these institutions. Actors who comply with these agendas are rewarded, while those who do not comply are punished in one form or another. The power embedded in international institutions is discussed at greater length in a later section of this chapter. Next, economic power can also be generated as part of the interdependence inherent to the global economy, in which states rely on

---

[209] Cox, Robert W. *Production, Power, and World Order: Social Forces in the Making of History*. New York: Columbia University Press, 1987. p.1.

[210] Cox, Robert W., and Timothy J. Sinclair. *Approaches to World Order*. Cambridge: Cambridge University Press, 2001. p.359.

[211] Nye, Joseph S. *The Future of Power*. New York, NY: PublicAffairs, 2011. p.52.

one another for a steady flow of trade, investment, and labour. In this framework, a state with greater economic power can often employ interdependence to its advantage. The ability to do this in part depends on "symmetry", which refers to situations of relatively balanced versus unbalanced dependence. As Nye notes, "Being less dependent can be a source of power. If two parties are interdependent but one is less so than the other, the less dependent party has a source of power as long as both value the interdependent relationship. Manipulating the asymmetries of interdependence is an important dimension of economic power."[212] The power embedded in interdependent economic relationships can be seen in the effectiveness of sanctions that utilize asymmetries in these relationships to achieve political objectives. Finally, economic power can be spawned as a consequence of a prosperous economy. This is crucial for providing the commodities and services necessary for the basic functioning and well being of a society, thereby decreasing overall tensions that can arise from economic malaise or poverty. The absence of a prosperous economy can in turn lead to an increase in social tensions that can be exploited by foreign adversaries to weaken the internal cohesion of a state.

Keeping in mind the centrality of the economy to the notion of state power, cyberspace has implications for the characteristics and functioning of the economy. Cyberspace has become an emerging domain for economic activity, competition, and wealth generation, and thus can contribute to the economic power of a nation. The cyber economy is estimated to be $4.2 trillion, the equivalent of 5.3 percent of GDP in G-20 economies, while in some of these countries the

[212] Nye, Joseph S. *The Future of Power*. New York, NY: PublicAffairs, 2011. p.55.

contribution of the cyber economy is as high as 8 percent of GDP.[213] It is estimated that the Internet economy has grown at an annual rate of 8 percent in the G-20 countries, outpacing all other economic sectors, between 2011 and 2016. The literature review has examined debates on the characteristics of the cyber economy, significance of cyberspace for economic development, and the negative side-effects of the uneven utilization of the cyber economy, including the digital divide between and within states. Chapter four will discuss and contribute to these debates in the context of Iranian cyberspace. The chapter will also examine and compare the cyber economy and the state of Information and Communication Technologies (ICT) development in the IRI to a set of sample countries in the Middle East, the Caucasus, and Central Asia regions.

2.1.3. Power embedded in International Institutions

International institutions have emerged as important actors on the global stage to address the plethora of pressing problems faced in common by states. Nye highlights that "in a world where borders are becoming more porous than ever to everything from drugs to infectious diseases to terrorism, nations must mobilize international coalitions and build institutions to address shared threats and challenges".[214] International institutions seek to promote the rule of law on the global stage, and create organizations and norms to change the conflictual nature of global politics by reducing states' "security dilemma" and fostering cooperation among states. Nye acknowledges structural-realist notions such as the significance of states in international relations and the anarchic nature of the international system, but argues that the prospects for cooperation, even in

---

[213] Dean, David, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'day, John Pineda, and Paul Zwillenberg. "The Internet Economy in the G-20." *The Boston Consulting Group (BCG)*. Mar. 2012. Web. 01 Mar. 2017. <https://www.bcg.com/documents/file100409.pdf>.

[214] Nye, Joseph S. *The Future of Power*. New York, NY: PublicAffairs, 2011. p.xvi.

an anarchical world, are greater than structural-realists suggest, and that inter-state cooperation can and should be organized and formalized in international institutions. According to Nye, the anarchy of the international system can be mitigated through international institutions which can increase the levels of regularity and predictability in international relations by broadening conceptions of self-interest, encouraging cooperation among states, formalizing expectations of states party to international agreements, overseeing compliance to international norms and regimes, and creating punishments for defectors.[215] Nye also diverges from structural realism when it comes to the question of how states perceive their interests. Structural realism contends that states focus on maximizing 'relative gains', or gains compared to rival states. In this worldview, states are unlikely to cooperate if they believe they will gain less than their rivals; they view the world as a 'zero sum game'. Meanwhile, Nye asserts that states focus on 'absolute gains', gains in and of themselves regardless of gains or losses of rival/partner states, making cooperation in international institutions feasible.[216]

Cox takes a somewhat different approach than Nye to the role of international institutions in international relations. He mirrors Nye in saying that international institutions are important in global politics and that states are no longer the sole actors. He underscores how the autonomy of the state has been much reduced by non-state actors, chief among them international institutions.[217] His ideas also parallel those of Nye when he states that international institutions

---

[215] Keohane, Robert O., and Joseph S. Nye. "Transgovernmental Relations and International Organizations." *World Politics* 27.01 (1974): 39-62.

[216] Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence: World Politics in Transition*. Boston: Little Brown, 1977. p.23-37.

[217] Cox, Robert O. "Realism, Political Economy and the Future World." *New Diplomacy in the Post Cold War World: Essays for Susan Strange*. Ed. Susan Strange, Roger Morgan, Jochen Lorentzen, and Anna Leander. New York, NY: St. Martin's, 1993. 27-44.

can often come up with solutions to global problems through cooperation, rather than conflict. Cox diverges from Nye, however, in arguing that international institutions can also serve as tools for the major powers: they embody a set of rules that typically facilitate, rather than hinder, the exercise of power by major powers on the global stage. Cox draws on the Gramscian idea of hegemony (discussed in detail in the following section) and asserts that: "One mechanism through which the universal norms of a world hegemony are expressed is the international organisation. Indeed, international organisation functions as the process through which the institutions of hegemony and its ideology are developed".[218] In other words, international institutions often represent the hegemonic states' ideology and values which shape the global order and reinforce their dominance and interests. Cox highlights that international institutions are often founded by major powers, and when they are not, the latter often exert influence over them through the provision of material support. Next, he stresses the ideological function of international institutions, pointing out how they "perform an ideological role as well. They help define policy guidelines for states and to legitimate certain institutions and practices at the national level."[219] This has the additional benefit of allowing major powers to become familiar with counter-hegemonic discourses, address certain aspects of them, and, by so doing, neutralize at least some of the threat they pose. Finally, international institutions socialize elites from states around the world, thereby exerting a more subtle level of influence on states through these individuals. Cox's solution is to expand the membership of international institutions beyond

---

[218] Cox, Robert W. "Gramsci, Hegemony and International Relations : An Essay in Method."*Millennium: Journal of International Studies* 12.2 (1983): 162-75. p.172.

[219] Ibid.

states to include genuine civil society organizations, which, through their participation and contribution, can help these institutions overcome these persisting issues.

As with coercive and economic power, it is inevitable that the exercise of power embedded in international institutions would, sooner or later, become enmeshed with cyberspace. In fact, the governance of cyberspace and issues surrounding it has become a subject of debate and contestation in international institutions. At the heart of the elevation of cyberspace to an issue to be addressed by international institutions is the strong tension between the non-territorial structure of cyberspace and territorially bounded state sovereignty. Cyberspace has parallels to trade and the environment as global issues in this regard, which, due to their inherently transnational nature, have spawned whole global institutions of governance.[220] The decision-making and agenda setting embedded in these institutions in turn constitute one of main aspects of exercise of power in cyberspace. These dynamics have already been discussed at length in the literature review. Chapter five examines the trajectory of the emerging regime of global Internet governance and the international institutions which produce and implement it, and how the IRI engages with these institutions to pursue its agenda within this regime.

2.1.4. Co-optive Power

The last major aspect of power articulated in the conceptualization of power by Cox and Nye is what has been referred to here as co-optive power. The latter is generated from ideational sources such as the attractiveness of political ideals and cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. Cox elaborates on the co-optive

---

[220] Mueller, Milton L. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

aspects of power following the Italian Marxist theorist Antonio Gramsci. The latter borrowed the notion of power as a centaur - the half-man half-horse of Greek legend - from Machiavelli to show how the ruling bourgeois capitalist class establishes and retains control. According to Machiavelli: "There are two methods of fighting, the one by law, the other by force: the first method is that of men, the second of beasts; but as the first method is often insufficient, one must have recourse to the second. It is therefore necessary to know well how to use both the beast and the man…and that the one without the other is not durable".[221] Based on the bifurcated Machiavellian concept of fighting, Gramsci argued that the ruling elite maintains its control through two types of power: "hegemony", which functions through consent that is created by civil society institutions and imposed on social life by the ruling class; and "direct domination," which operates through the coercive power of the state and "legally" disciplines those forces which actively or passively refuse to consent.[222] Gramsci gives us a historical example to illustrate this point: "When the pressure of coercion is exercised over the whole complex of society (and this has taken place in particular since the fall of slavery and the coming of Christianity) puritan ideologies develop which give an external form of persuasion and consent to the intrinsic use of force".[223] He emphasizes that ruling elites always try to combine force and consent, and often try to veil force under the mantle of popular consent.

Therefore, we cannot meaningfully limit our definition of power to the coercive power of the "State" and "political society", which "legally" enforce discipline on the people. Rather, we must

---

[221] Machiavelli, Niccolò. "The Prince." *Princeton Readings in Political Thought: Essential Texts since Plato*. Ed. Mitchell Cohen and Nicole Fermon. Princeton, NJ: Princeton University Press, 1996. 167-87. p.183.

[222] Gramsci, Antonio. *Selections from the Prison Notebooks of Antonio Gramsci*. Trans. Quintin Hoare and Geoffrey Nowell-Smith. New York, NY: International, 1971. p.12.

[223] Ibid.. p.299.

extend our definition to include “hegemony” deriving from the private apparatuses of civil society, which are conceived of as being embodied in concrete historical institutions. According to Cox these institutions include “the church, the educational system, the press, all the institutions which helped to create in people certain modes of behavior and expectations consistent with the hegemonic social order”.[224] In this sense, Gramsci’s definition of power is based on a dialectical relationship between the sphere of civil society, consent and hegemony, on one hand, and State or political society, force, and direct domination on the other. Cox extends this Gramscian conceptualization of power beyond domestic politics to analyze the “international power relations or world order”, arguing that hegemony at the global level is not merely achieved through coercive power, but also the triumph of a hegemonic state's ideology and values.[225] This happens at the level of international institutions which, as discussed above, can serve an ideological function in terms of defining policy guidelines and legitimating certain institutions and practices for states that favour the interests of major powers.

Cox distinguishes between direct coercive means, on one hand, and indirect non-coercive means, on the other, demarcating these as two opposite ends of a spectrum. In *Bound to Lead*, Joseph Nye condensed this spectrum into two concrete notions of power: hard and soft power.[226] Hard power is defined as the use of coercion or payment. Soft power, resting on the other end of the power spectrum, relies on the ability to frame agendas, attract, and convince.[227] Here coercion or

---

[224] Cox, Robert W. "Gramsci, Hegemony and International Relations : An Essay in Method."*Millennium: Journal of International Studies* 12.2 (1983): 162-75. p.164.

[225] Ibid.. p.169.

[226] Nye, Joseph S. *Bound to Lead: The Changing Nature of American Power*. New York: Basic, 1990.

[227] Nye, Joseph S. *Soft Power the Means to Success in World Politics*. New York: PublicAffairs, 2004.

payments refers to the more well established and conventional idea of power, which grows out of a country's economic and military strength. Soft power, in contrast, comes from "the attractiveness of a country's culture, political ideals, and policies", what Nye collectively calls a country's primary currencies.[228] Accordingly, Nye points out that the sources of soft power are not monopolized by governments to the same extent that hard power is, but are largely produced by "societal forces outside government control".[229] Critiquing the materialist and coercive conceptualization of power in structural realism, Nye argues: "It is also important to set the agenda and attract others in world politics, and not only to force them to change by threatening military force or economic sanctions. This soft power – getting others to want the outcomes that you want – co-opts people rather than coerces them." Nye emphasizes that soft power should not be dismissed as merely "a question of image, public relations, and ephemeral popularity",[230] but rather as a distinct type of power which can be used to achieve one's ends:

> Political leaders and thinkers such as Antonio Gramsci have long understood the power that comes from setting the agenda and determining the framework of a debate. The ability to establish preferences tends to be associated with intangible power resources such as an attractive culture, ideology, and institutions. If I can get you to want to do what I want, then I do not have to force you to do what you do not want to do.[231]

The elaborations of Cox and Nye on co-optive aspect of power thus expand the concept of power beyond material-coercive factors to include ideational-persuasive factors. Crucially, as Cox and Nye pinpoint, the sources of coercive power (the military and police) are generally controlled by

---

[228] Ibid.. p.x.

[229] Nye, Joseph S. *Power in the Global Information Age: From Realism to Globalization*. New York, NY: Routledge, 2004. p.91.

[230] Nye, Joseph S. *Soft Power the Means to Success in World Politics*. New York: PublicAffairs, 2004. p.129.

[231] Nye, Joseph S. *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone*. Oxford: Oxford University Press, 2003. p.9.

the states, whereas the sources of co-optive power (culture, political ideals, policies, institutions, etc.) are mainly in the hands of civil society.

Co-optive power is potentially most relevant in cyberspace.[232] The millions of people who are both audience and actors in cyberspace can act in favor of or against a state's interests based on its co-optive power.[233] Governments can exercise co-optive power over civil society by promoting their own political ideals and cultural values in cyberspace, legitimizing their policies in the eyes of citizens. On the other hand, civil society organizations can use the very same domain to promote the political ideals and cultural values at odds with that of the state, countering the state's co-optive power. In the long-term, this can result in the loss of influence and legitimacy of the IRI's own culture and political ideals among Iranians. The sense of threat felt by IRI officials from their domestic and foreign rivals' exercise of co-optive power is best illustrated by Supreme Leader Ayatollah Ali Khamenei:

> Everyone today understands and knows that the confrontation between the Arrogance and the Islamic Republic regime is no longer like the confrontation of the first decade of the revolution. In that confrontation they exercised their power, and were defeated. That confrontation was a *hard* confrontation… However today this is not the priority of the Arrogance for confronting the Islamic regime. The priority today is what is called *soft* war; that is war using cultural tools, through infiltration of our society, through lies, through spreading rumors. Through the advanced instruments that exist today, communication tools that did not exist ten, fifteen, and thirty years ago, have become widespread. *Soft war means creating doubt in people's hearts and minds.* [234]

---

[232] Keohane, Robert O., and Joseph S. Nye. "Power and Interdependence in the Information Age." *Foreign Affairs* 77.5 (1998): 81-94.

[233] Nye, Joseph S. *Power in the Global Information Age: From Realism to Globalization*. New York, NY: Routledge, 2004.

[234] Khamenei, Ali. "Bayanat Dar Jam-e Kasiri Az Basijian-e Keshvar (A Speech to a Large Crowd of the Nation's Basij)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei*. 25 Nov. 2009. Web. 26 Oct. 2017. <http://farsi.khamenei.ir/speech-content?id=8430> (Emphasis added).

As demonstrated in the quote, the IRI's political elite, specifically the principlist/conservative political current in charge of the majority of the unelected centers of power in Iran, claims that the IRI's cultural and political ideals are mainly confronted by the Arrogance (*Estekbar*), a term referring to the IRI's foreign rivals, namely the United States. The reality, however, is that domestic 'primary currencies' generated by Iranian social movements, Islamic and secular scholars and intellectuals, and progressive clergy in Islamic seminaries, among others, widely utilize cyberspace to critique the cultural and political ideals of the IRI and promote alternative 'primary currencies', extracted from the rich reservoir of pre-Islamic and Islamic Iranian culture and history. In other words, if there is an ongoing soft confrontation, it is largely between the IRI and Iranian civil society, rather than the IRI and its foreign adversaries. However, this does not mean that states do not try to affect public opinion in other states by distributing their own primary currencies in order to achieve their objectives. As already noted in the literature review, cyberspace is a new domain for conducting public diplomacy and increases the speed at which primary currencies can be distributed and the depth to which they can penetrate. In an interconnected world, states at once attempt to preserve their own primary currencies and at the same time distribute it to affect others. While some willingness exists on the part of the IRI to conduct cyber public diplomacy abroad, it has not yet taken serious steps in this direction, as already shown in the literature review. At the domestic level, the initial response of the IRI has been to employ coercion to block the distribution of rival primary currencies within Iran, discussed at length in chapter three. Over time, however, its approach has evolved as it has found that coercion alone is insufficient to block the entry and effectiveness of rival primary currencies. Instead in more recent years it has attempted to use cyberspace to deploy its own primary currencies and ideational factors to compete with those of its rivals, discussed in detail in chapter six.

2.2. Research Design

In the novel domain of cyberspace, we are faced, on the one hand, with the physical and non-physical infrastructure, the hardware and software, which underpin information communication in cyberspace. On the other hand, we have the set of social relations made up of a mass user base shaping and being shaped by this domain. This dualistic nature of cyberspace poses challenges about which methodological approach, quantitative or qualitative, is best suited to answering the question animating this research. As King, Keohane and Verba argue, the majority of research does not neatly fall into one category or the other, with the best combining quantitative and qualitative methods in a complementary way, and each canceling out the weaknesses of the other.[235] The following sections will show how this hybrid approach, combining elements of both qualitative and quantitative methods, is especially desirable in conducting a case-study of the measures the IRI has taken in cyberspace and their interaction with Iranian state-society and international relations.

2.2.1 Research Method: The Rationale and Relevance of a Single Case Study of the IRI

This dissertation uses the single case study method to understand the measures the IRI has taken toward cyberspace of policies toward cyberspace and their interaction with Iranian state-society and international relations. The rationale for a single case study emerges from the particular characteristics of Iranian cyberspace and the uniqueness of the IRI in experiencing the full-range of opportunities and risks associated with the diffusion of power in cyberspace in a way which not many states have to date. The IRI has experienced a rapidly rising rate of Internet usage over

[235] King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press, 1994.

the last few years, with the number of users having grown by 50 percent since 2000, higher than any other country in the Middle East. Internet users account for nearly 31.3 percent of Iran's population, considerably higher than the Middle East average of 23 percent.[236] This high Internet penetration-rate, combined with Iran's young and vibrant population and a number of other factors led a Human Rights Watch report to conclude that: "Iran has the potential to become a world leader in information technology. It has a young, educated, computer-literate population that has quickly taken to the Internet. It is rapidly developing its telecommunication infrastructure".[237] A second factor further compounds the appropriateness of this case study. As Sreberny and Khiabany have noted, given the IRI's control of the traditional media and political space, much of Iranian society's media and political activity has moved into cyberspace, whose characteristics make it an ideal place for this activity to play out: "Thus, the internet became the space for political debate when other fora such as the press and face-to-face embodied politics became suppressed. Indeed, by keeping people indoors with little to do but fiddle with computers, the regime helped to induce a generation of digital adepts, the consequences of which it was to rue in the summer of 2009".[238]

The IRI's unique experience with cyberspace is also a key consideration for its selection for this case study. Its experience gives us many examples of risks and opportunities to choose from. The Stuxnet worm, which targeted industrial systems underlying the Iranian nuclear program and

---

[236] Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT, 2010. p.547.

[237] Salhi, Hamoud. "Assessing Theories of Information Technology and Security for the Middle East." *International Relations and Security in the Digital Age*. Ed. Johan Eriksson and Giampiero Giacomello. London: Routledge, 2007. 106-31. p.125.

[238] Sreberny, Annabelle, and Gholam Khiabany. *Blogistan: The Internet and Politics in Iran*. London: I.B. Tauris, 2010. p.116.

specifically its uranium enrichment infrastructure, is a prime example of a cyber risk posed by one state against another on the international level.[239] This cyber attack has allegedly made the IRI the *first known victim of cyber warfare* by a global hegemon, the United States, and its ally, Israel.[240] The attack, first publicly revealed in 2010, is said to have destroyed 1000 out of 9000 centrifuges at Iran's Natanz uranium enrichment facility.[241] The computer security firm F-Secure Lab has estimated that over ten man years of time went into developing Stuxnet, including for research, exploration, and testing in a mirrored environment.[242] Since 2010, a number of other worms beside Stuxnet have been detected attacking Iran and other Middle Eastern states, including Duqu, Flame, and miniFlame.

The Green Movement, which utilized cyberspace as the key element of its communication strategy and threatened the political stability of the IRI, is another example of a cyberspace risk but one posed by Iranian people on the domestic-level. Websites and blogs as well as newer Web 2.0 applications, such as YouTube and Twitter, were the most ubiquitous communication instruments in the movement, making "it possible for news to flow from Iran despite government censorship of the Internet and bans on foreign media coverage".[243] Some scholars, including

---

[239] Matsubara, Mihoko. "A Stuxnet Future? Yes, Offensive Cyber-Warfare Is Already Here."*Center for Security Studies*. ETH Zürich, 23 Oct. 2013. Web. 20 Oct. 2017. <http://www.css.ethz.ch/en/services/digital-library/articles/article.html/154091/pdf>.

[240] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown, 2014.

[241] Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report." *Institute for Science and International Security*. 15 Feb. 2011. Web. 05 June 2017. <http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf>.

[242] Aquilino, Broderick, Et al. *F-Secure Labs*. 2012. Web. 01 Oct. 2017. <https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2012.pdf>.

[243] Yahyanedjad, Mehdi, and Elham Gheytanchi. "Social Media, Dissent, and Iran's Green Movement." *Liberation Technology: Social Media and the Struggle for Democracy*. Ed. Larry Diamond and Marc F. Plattner. Baltimor, Md: John Hopkins University Press, 2012. 139-53. p.140.

Hamid Dabashi, have argued that cyberspace in general and social networking in particular were "fundamental" aspects of the Green Movement: "The skeletal structure of cyberspace, well-oiled and operative due to mundane use, was now instantly turned into an effective mechanism of social mobilization, political opposition, and generation of dissent".[244] This estimation of the importance of the Internet to the Green Movement, is echoed by Charles Kurzman: "electronic media have been one of the backbones of the Green Movement".[245] The fundamental role of cyberspace in the Green Movement led many to call these demonstrations "Iran's Twitter Revolution", and some go so far as to say that "Twitter and its creators are worthy of being considered for the Nobel Peace Prize".[246] The continued relevance of this experience was recently confirmed by the Iran protests of December 2017 and January 2018. During these protests, the tens of thousands of participants used the widely popular Telegram messaging application to communicate and organize across over 70 cities. This posed such a challenge to Iranian authorities that they felt compelled to temporarily filter Telegram.

On the other hand, the IRI has found opportunities in cyberspace to exercise power at the international level. Following the 2009 demonstrations, a group labeling itself as the Iranian Cyber Army commenced a campaign of harassment against Green Movement activists and sympathizers inside Iran and abroad. These online attacks became prevalent as a tool used by the IRI and its supporters in order to create a climate of fear and suspicion among Green Movement

---

[244] Dabashi, Hamid. *Iran, the Green Movement and the USA The Fox and the Paradox*. London: Zed, 2010. p.136.

[245] Kurzman, Charles. "Cultural Jiu-Jitsu and the Iranian Greens." *The People Reloaded: The Green Movement and the Struggle for Iran's Future*. Ed. Nader Hashemi and Danny Postel. Brooklyn, NY: Melville House, 2010. 7-17. p. 7.

[246] Pfeifle, Mark. "A Nobel Peace Prize for Twitter?" *The Christian Science Monitor*. 06 July 2009. Web. 01 Oct. 2017. <http://www.csmonitor.com/Commentary/Opinion/2009/0706/p09s02-coop.html>.

activists and supporters and weaken them.[247] Noteworthy successful operations by the Iranian Cyber Army included defacement of social networking, news, and governmental websites such as Twitter and Voice of America, among others, by covering their pages with pro-IRI slogans and their logo.[248] Such attacks emboldened the IRI publicly, with official government spokesperson Ali Saeed Shahroudi saying that the United States could no longer say that it was the "bellwether of software and cyber technology".[249] Even Google, the reigning titan of the U.S. tech industry, did not prove immune to Iranian cyber-operations, reporting on 29 August 2011 that sophisticated attacks from Iran on its certificate authority systems securing online traffic into and out of Iran. These attacks led Google Executive Chairman Eric Schmidt to tell CNN that: "Iranians are unusually talented in cyber warfare for some reason we don't fully understand… The Iranians are clearly a cyber security threat in our future."[250] In 2011, General Gholam-Reza Jalali, head of the Civil Defense Organization of Iran (CDO), welcomed "hackers who are willing to work for the goals of the Islamic Republic with good will and revolutionary activities".[251] On 20 February 2012, he officially declared that the IRI had begun to operate its first cyber army,[252] and just a few months later the IRI allegedly brought the Saudi Arabian national oil company's information systems under intense attack.[253]

---

[247] Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013. p.166.

[248] Ide, William. "Iranian Hackers Attack VOA Internet Sites." *Voice of America (VOA)*. 22 Feb. 2011. Web. 05 June 2017. <https://www.voanews.com/a/iranian-hackers-attack-voa-internet-sites-116678844/172741.html>.

[249] Ibid.. p.167.

[250] CNN. "Google's Eric Schmidt on Protecting America's Tech Secrets." *CNN*. 13 Dec. 2011. Web. 05 June 2017. <http://outfront.blogs.cnn.com/2011/12/13/googles-eric-schmidt-on-protecting-americas-tech-secrets/>.

[251] Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013. p.167.

[252] Press TV. "'Iran Set to Build First Cyber Army'." *Press TV*. 20 Feb. 2012. Web. 05 May 2017. <https://web.archive.org/web/20120621015437/http://www.presstv.ir/detail/227739.html>.

[253] Bronk, Christopher, and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco."*Survival* 55.2 (2013): 81-96.

Likewise, cyberspace has provided the IRI with greater opportunities for surveilling its domestic population, giving it access to a higher quality and quantity of personal information than was possible in the past. Beginning in 2009, the IRI started requiring all private Internet service providers (ISPs) offering Internet connectivity services to the public to connect online through the state-owned Telecommunication Company of Iran (TCI).[254] This means that all Internet traffic goes through a single, government-controlled, pathway, allowing the state to conduct extensive surveillance of the public's online activities, including monitoring of online social networks and finding the locations of and targeting specific online activists and users. Looking at the IRI's cyber policing activities, Anthony H. Cordesman has argued that: "A task force of 250,000 cyber police currently monitors the Internet, specific sites, blogs and individuals suspected of using circumvention tools".[255] There is considerable controversy concerning the IRI's cyber policing activities, as with China, given that much of its technical capability is provided or at least complemented by hardware and software sold by European and other foreign companies.[256]

2.2.2 Data collection and analysis

This dissertation will use the following methods for collecting quantitative and qualitative data:

2.2.2.1. Online public documents (primary sources): Publicly available online documents, including from government archives and repositories, have been reviewed. These include four categories of documents. The first category includes executive orders, parliamentary laws, and

---

[254] Abdo, Geneive. "The New Political Tools." *The Iran Primer: Power, Politics, and U.S. Policy*. Ed. Robin B. Wright. Washington, D.C: United States Institute of Peace, 2011. 53-56.

[255] Cordesman, Anthony H. *The Gulf Military Balance: The Conventional and Asymmetric Dimensions*. Washington, D.C.: Center for Strategic and International Studies, 2014. p.172.

[256] Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT, 2010.

judicial commands setting out the country's cyber policies and regulations in a wide-range of fields, such as the National Information Network (NIN), regime of cyber filtering, body of law regulating cyber activities, and defensive and offensive measures taken by the IRI to exercise coercive power in cyberspace against foreign rivals. The second category includes all available documents pertaining to the IRI's involvement in global events on Internet Governance. In cases when IRI delegates to these global events referred to the contribution of other parties, the documents of these parties were also incorporated. In the same vein, outcome documents of these global events were assessed to understand the extent to which the IRI's views were reflected in them. The third category includes reports by leading governmental organizations in the IRI, including the Supreme Council of Cyberspace (SCC), the Civil Defense Organization (CDO), Cyberspace Research Institute (CRI), and Committee to Determine Incidences of Criminal Content in cyberspace (CDICC). Finally, the fourth category assembles the speeches and interviews of Iran's leading officials with authority over cyberspace in Iran, including Information and Communication Technology ministers, the heads of Civil Defense Organization, the commanders of Cyber Police of Iran, and the members of Supreme Council of Cyberspace head.

2.2.2.2. Academic literature on cyberpolitics (secondary sources): A critical review of the academic literature on the implications of cyberspace for state-society and international relations in general, and Iranian case in particular, has been conducted. At the level of state-society relations, this includes the literature on the impact of cyberspace on social mobilization, collective action repertoires, and media coverage. This also includes the literature on how states adopt measures such as propaganda, surveillance and denial of access in order to maintain their control over cyberspace. At the level of international relations, the academic literature used in

this dissertation is mainly centered on the measures adopted by states to secure the critical infrastructure of cyberspace, Internet economy and ICT development, Internet governance, and public diplomacy.

2.2.2.3. Semi-structured interviews: In-depth and semi-structured interviews have been conducted with individuals with knowledge and expertise on Iranian cyberspace and/or the IRI's measures in cyberspace. An interview was conducted with Amir Rashidi, a researcher at the International Campaign for Human Rights in Iran who focuses on Iranian cyberspace both at the policy and technical level. Mr. Rashidi, who resided in New York City at the time of the interview and spoke with me over several sessions via Skype, also has experience within Iran as a senior official in electoral campaigns including that of Mehdi Karroubi in the 2009 presidential election. An interview was conducted with a former senior IRI official, who asked to remain anonymous. His position was in the area of ICT policy and development and responded to questions in writing over email. There was also an attempt to speak with two social activists who utilize cyberspace to propagate their ideas and interact with their target audience. Preliminary preparations were completed, including receiving their consent to be interviewed. Their participation in this research ultimately ended, however, for security reasons in light of the recent Iranian protests of December 2017 and January 2018.

2.2.2.4. Raw technical and macro-economic data: Data from the indexes listed below have been used to examine and compare the development of the cyber economy in the IRI to other countries in the Caucasus, Central Asia, and Middle East regions. This data covers the period between 2002 and the present. These indexes include: 1) The Economist Intelligence Unit and IBM Institute for Business Value's E-readiness Index (ERI); 2) The United Nations' E-

government Development Index (EGDI); 3) The World Economic Forum's Networked Readiness Index (NRI); and 4) The International Telecommunication Union's ICT Development Index (IDI).

2.2.2.5. Quantitative and qualitative social media data: Data was extracted from the two major social media platforms utilized in Iranian cyberspace, Telegram and Instagram, to examine quantitatively the level of activity and influence of the top figures involved in the generation of ideational factors and to analyze qualitatively the content they produce.

Conclusion

The opening of this dissertation, including the introduction and literature review chapters, demonstrated that cyberspace is not merely a technical phenomenon but a domain in which power can be exercised and impact state-society and international relations. In order to understand how this power is exercised and impacts politics, we need a workable conceptualization of power that corresponds with the different facets of cyberspace. This chapter conceptualized power in the framework of the discipline of International Relations because of the inherently global nature of cyberspace, in which territorial boundaries are not a barrier to the ability of actors, both at the domestic and global level, to influence one another. It was shown that power has generally been conceptualized in line with dominant realist interpretation of power, which is based on coercion, state-centrism, and materialism. The chapter then showed how International Relations scholars Robert W. Cox and Joseph S. Nye accepted this basic premise, but went beyond it to introduce a synthetic concept of power that highlighted the non-coercive dimensions of power, the role of non-state actors, and significance of ideational factors in politics. These thinkers give an alternative conceptualization of power that is more

comprehensive and nuanced when compared to structural realism, distinguishing between what they viewed as the four major dimensions of power: coercive, economic, institutional, and co-optive. By incorporation state-society relations, this conceptualization is also versatile enough to provide insights into how power is exercised at the level of domestic politics.

This chapter showed that this multifaceted conceptualization of power provides us with a useful tool to examine the exercise of power in cyberspace and its impact on state-society and international relations. The first dimension explains the measures adopted by states to exercise coercive power in cyberspace at the domestic level, including a: national information network; comprehensive regime of filtering; and laws regulating cyber activities and the law enforcement organizations that implement them. This same dimension helps elucidate defensive and offensive cyber measures taken by states against foreign adversaries. The second dimension lays out the measures adopted by states to develop their Information and Communication Technologies (ICTs) to exploit the huge economic potential of cyberspace. The third dimension illuminates the measures taken by states to govern cyberspace through international institutions of Internet governance. Finally, the fourth dimension elaborates on the utilization of cyberspace by state and non-state actors both at the domestic and global level to propagate their favored political and social agenda, while countering that of their adversaries by generating and debating different ideational factors associated with political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. Each of these dimensions in the context of Iranian cyberspace will be examined at length in chapters three through six.

This chapter showed that social relations and technical infrastructure, which make up the two main aspects of cyberspace, have together produced a wide variety of data. This motivated the

research design of this dissertation which is composed of a hybrid methodological toolbox suitable for collecting both quantitative and qualitative data, including: online public documents, the academic literature on cyberpolitics, semi-structured interviews, raw technical and macro-economic data, and social media data.

The theoretical framework and methodology presented in this chapter constitute the foundation of our case study, which begins in the next chapter.

CHAPTER THREE: IRAN AND THE EXERCISE OF COERCIVE POWER IN CYBERSPACE

Introduction

As discussed in the literature review, cyberspace affects state-society relations by aiding social actors through three main mechanisms: first by facilitating mobilization; second, by expanding and updating collective action repertoires of contention; and third, by granting the ability to generate and frame favorable media coverage independent of big (state and corporate) media. In the same chapter, it was explained how these mechanisms help social actors, including social movements, criminal organizations, and militant groups, to challenge the state to reach their goals, and thus can pose a security threat at the domestic level. Cyberspace also influences international relations because it is a new domain in which actors can carry out hostile actions toward one another to advance their political goals, namely through cyber-attacks, -espionage, and -terrorism. How do states respond to such real and perceived cyber threats, both at the level of state-society and international relations? States often respond to such threats by exercising coercive power, one of the principal dimensions of power discussed in the theoretical framework. The main feature of this aspect of power is to impose one's will over another through coercion, or the utilization of what Robert W. Cox calls destructive material capabilities and Joseph S. Nye calls hard power.

This chapter examines the four main pillars through which the IRI exercises coercive power in cyberspace to confront these real or perceived threats. Section one studies the National Information Network (NIN) project and the conditions under which this project constitutes a pillar of coercive power by limiting access to the global Internet for Iranian society and

potentially compromising the cyber security of Iranian users. Although initially established as a national intranet to isolate Iranian cyberspace from the larger global Internet, the goals of the NIN have evolved away from its coercive origins as a result of a combination of the change in presidential administration and technical difficulties faced by the IRI in implementing the project. Section two examines the comprehensive regime of filtering as a pillar of coercive power in the context of the IRI's general approach to limiting Iranian society's access to information. This section explores the evolution and characteristics of the filtering regime, the development of different institutions to oversee and administer it, and how the structural tensions between these institutions impact the implementation of Internet filtering in Iran. The third section looks at the Iranian body of law regulating cyber activities and the main law enforcement organizations created for its implementation as one of the main pillars of coercive power used by the IRI to deter activities it deems undesirable in cyberspace. This section divides the cyber activities that are punishable under the law into four socio-cultural, political, security, and cyber criminal categories. The most restrictive elements of this body of law can be found in the first two categories, both due to the breadth of the activity they cover and severity of the punishments they entail. Section four looks at the defensive and offensive measures taken by the IRI to exercise coercive power in cyberspace against its foreign rivals. The section explores the IRI's defensive measures in the context of the cyber attacks conducted against it by rival state actors since 2009, making it among the first victims of coercive action in cyberspace by one state against another. The section also elaborates on the offensive measures adopted by the IRI to demonstrate its capability to retaliate against its rivals and establish deterrence. The chapter concludes by summarizing its findings and examining the effectiveness of the IRI's coercive approach to cyberspace.

3.1. The National Information Network

The National Information Network (NIN), which in the past has also been labelled the National Internet, Halal Internet, and Clean Internet, is a national intranet that, when completed, will be largely isolated from the global Internet. The infrastructure of the NIN, including routers, switches, and data centers, will be completely based in Iran, and house important domestic networks and websites, such as those belonging to the government and research and educational centers.[257] This ambitious ICT project can potentially be used by the IRI as a means of coercion to limit access to the global Internet for Iranian society and compromise the cyber security of Iranian users.

The initial plans for the NIN emerged under the presidency of Mahmoud Ahmadinejad after his Cabinet approved the project in early 2006, slating it for completion within three years.[258] At the time the project seemed to be one viable solution to the dilemma of Internet development in Iran. While the huge economic potential of the Internet for economic development could simply not be ignored, the IRI leadership was disturbed by the proliferation of online content which it deemed not to conform with the political ideals and cultural values of the Islamic Republic. The original response to this dilemma was to implement a comprehensive regime of filtering to prevent undesired content from being consumed by Iranians. The leadership decided that an intranet in which undesirable content would not be generated in the first place was a better and

---

[257] SM. "Internet Infrastructure and Policy Report - March 2014." *Small Media*. Mar. 2014. Web. 01 June 2017. <https://www.smallmedia.org.uk/old/content/114.html>. p.3.

[258] NCC. "Shabakeh-ye Malli-ye Ettelaat (The National Information Network)." *The National Center of Cyberspace*. The Supreme Council of Cyberspace, 26 June 2016. Web. 02 June 2017. <http://majazi.ir/page/national-information-network>.

viable alternative to filtering alone.[259] This was called the Halal Internet, with the term "Halal" denoting permissibility and ritual purity of an action in Islam. While the three year deadline set by the Iranian Cabinet to complete this project was already ambitious, just a few months later Mohammad Soleymani, then minister of communication and information technology, announced the preliminary phase of the NIN would be available by October 2006.[260] Unsurprisingly, this time frame was not realistic and passed, and the NIN project saw no real progress even by the original three year deadline.

After almost five years of very sluggish progress, the NIN project was accelerated in 2011 when it formally became a national priority under Article 46 of the Fifth Five Year Development Plan (2011-2016).[261] According to the plan, NIN infrastructure consists of data centers located inside the country whose data is not accessible from abroad. Furthermore, when domestic users request data located in these data centers, their traffic will not go through the global Internet, but instead remain in networks that are within Iranian national boundaries. The plan tasks the ICT ministry with implementing the NIN based on "religious and security" criteria and commits that by its second year all governmental organizations should be connected to the NIN and that their communication be exclusively conducted on its networks. By 2016, the plan had called for all public services to be offered on the NIN as well as for 60 percent of families and businesses also be connected to the network.

---

[259] Amir Rashidi, interview by author.

[260] FNA. "Goftegu-ye Tafsili-ye Fars Ba Vazir-e Ertebatat Va Fanavari Ettelaat (Fars' Extensive Conversation with the Minister of Communication and Information Technology)." *Fars News Agency*. 23 July 2006. Web. 01 June 2017. <http://www.farsnews.com/8505010040>.

[261] IPRC. "Ghanun-e Barnameh-ye Panjsaleh-ye Panjom-e Tose-ye Jomhuri-ye Eslami-ye Iran (1390-1394) (Fifth Five Year Plan of the Islamic Republic of Iran (2011-2015))." *Islamic Parliament Research Center of the Islamic Republic of Iran*. 20 Jan. 2011. Web. 01 June 2017. <http://rc.majlis.ir/fa/law/show/790196>.

This renewed drive to complete the NIN was primarily motivated by two events: The 2009 Green Movement demonstrations and 2010 Stuxnet cyber attack. The Green Movement had placed the IRI leadership in a difficult predicament. While shutting down domestic access to the Internet would have deprived demonstrators of their primary means of communication, it would also have come at a tremendous cost to the country's economy. Inaction, on the other hand, risked allowing the Green Movement to continue to utilize cyberspace as the main tool in its communication and mobilization strategy, allowing further challenge to the state's authority.[262] While the IRI chose shutting down access to the Internet, it did so with some reluctance and at great cost. The second event was the Stuxnet attack, believed to have been a joint U.S.-Israeli cyber operation, which did enormous damage to centrifuges at the Natanz Fuel Enrichment Plant.

When completed, the NIN will enable the IRI to better deal with both domestic tumult and foreign cyber operations. Contrary to the predicament it faced with the Green Movement in 2009, in the future the IRI will be able to confront similar demonstrations by shutting off access to the global Internet without incurring the same economic costs this would normally entail, because domestic networks in the NIN would continue to operate.[263] The NIN is also supposed to make the execution of foreign cyber operations against Iran more difficult. Interestingly, had the NIN existed in 2010 it would not have prevented the Stuxnet attack.[264] This is because this operation was not conducted through foreign remote infiltration of Iranian systems via the global Internet, but rather through local access: An individual inserted an infected USB flash drive

---

[262] Safshekan, Roozbeh. "The Matrix of Communication in Social Movements: A Comparison of the 1979 Revolution and 2009 Green Movement in Iran." *Sociology of Islam* 2.3-4 (2014): 328-45.

[263] Amir Rashidi, interview by author.

[264] Amir Rashidi, interview by author.

directly into the network at Natanz.[265] Nonetheless, the NIN would provide Iranian networks a much higher level of security against foreign cyber operations.

While the NIN project was supposed to be completed within the timeframe of the Fifth Five Year Development Plan, it saw very little progress under Ahmadinejad and fell behind schedule, a delay which could be attributed to two primary reasons. First, the NIN is a technically complex and large-scale project which has been achieved in virtually no other country, even those with a high level of scientific and technological infrastructure. Another reason was the comprehensive regime of international sanctions against Iran because of its nuclear program, which made the importation of technology necessary for the implementation of the NIN difficult.[266] The cumulative effect of these obstacles was that during the final two and a half years of the Ahmadinejad administration, which overlapped with the first half of the Fifth Five Year Development Plan, the NIN project saw very little concrete progress and one missed deadline after another.

Given these limits on the ability of the IRI to advance the infrastructure of the NIN, the Iranian government shifted toward developing a variety of indigenous softwares which could be deployed on this infrastructure once it is completed. This includes the Xamin and Ghasedak operating systems released in 2012.[267] At the time of writing, however, the available data

---

[265] Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers, 2014.

[266] Amir Rashidi, interview by author.

[267] MNA. "Joziat-e System-e Amel-e Bumi-e Xamin (Details of the Indigenous Xamin Operating System)." *Mehr News Agancy*. 23 June 2012. Web. 01 June 2017. <http://www.mehrnews.com/news/1632002>. and, Gerdab. "System Aml-e Bumi-ye Ghasedak Eraeh Shod (Indigenous Ghasedak Operating System Is Released)." *Gerdab*. Center for the Investigation of Organized Cybercrimes (CIOC), 28 Aug. 2012. Web. 01 June 2017. <http://www.gerdab.ir/fa/news/12033>.

suggests Ghasedak has been quite unsuccessful compared to foreign alternatives like Windows based on both functionality and security, while the Xamin website is altogether inaccessible, suggesting it is no longer being offered. According to the most recently available data from the ICT ministry, as of 2015 there were 12994720 families in Iran with access to a personal computer.[268] Compare this to statistics available on the Ghasedak website which indicate that there were 89215 total downloads of this operating system, suggesting a maximum adoption rate of 0.7 percent.[269] The national adoption rate is likely far lower when we consider that each household may have more than one computer and if we include all computers from the government and private sector. In January 2011 the ICT minister called for the creation of a national operating system "document" which would make use of the domestic operating systems mandatory by law.[270] However, there have been no developments in this regard, and in the absence of such coercive measures to make use of government software obligatory, these operating systems are likely to remain largely unused.

The same trend can be observed in the development of indigenous search engines. The two most prominent examples of these are Parsijoo, whose fourth edition was released in February 2015, and Yooz, which after being in development for five years became functional during the same

---

[268] MISI. "Vaziat-e Tose-ye Fanavari-ye Ettela'at Va Ertebatat Keshvar (The Country's State of Information and Communication Technology Development)." *The Official Portal of Measuring Information Society of Iran*. Ministry of Information and Communications Technology of Iran, 2015. Web. 01 Mar. 2017. <http://mis.ito.gov.ir/documents/20182/34805/ict94/63cb5ef2-982e-4fbc-9c81-120a0a83e765>.

[269] Ghasedak. "Download-e System-e Amel-e Bumi-ye Ghasedak (Indigenous Ghasedak Operating System Download)." *Markaz-e Poshtibani-ye Online Ghasedak (Ghasedak Online Support Center)*, 1 Sept. 2012. Web. 01 June 2017. <http://support.qsdk.com/index.php?_m=downloads&_a=viewdownload&downloaditemid=110&nav=0>.

[270] MNA. "Mosahebeh-ye Mehr Ba Vazir-e Ertebatat Va Fanavari Ettelaat (Mehr's Interview with the Minister of Communication and Information Technology)." *Mehr News Agency*. 04 Jan. 2011. Web. 02 June 2017. <http://www.mehrnews.com/news/1224464>.

month.[271] Alexa, a website which rates websites according to use for each country, ranked Google search engine as the top website in Iran as of 2 June 2015, while Parsijoo was ranked #391 and Yooz #2402.[272] Despite this abysmal performance after millions of dollars of investment in these search engines, the ICT ministry announced on May 2015 that they would provide both projects with an additional 170 billion toman (70 million dollars) in order to help them improve their positions in the Iranian search engine market.[273]

A comparable, if slightly different pattern can be observed with the development of indigenous web browsers. The most prominent example of this is the Saina browser, developed by the ICT ministry and finally released in October 2013.[274] This browser is supposed to compete with popular browsers such as Firefox, Chrome, Safari, and Internet Explorer. However, a closer look reveals that Saina is a modified version of the Firefox browser that is not necessarily an improvement on the original when it comes to security and other issues.[275] For example, accessing the Library, Museum and Document Center of the Islamic Consultative Assembly of Iran website using Firefox, Chrome, and Safari prompts a warning that going to the website risks

---

[271] TNA. "Motor-e Jostejugar-e Parsijoo Dar Yazd Runamayi Shod (Parsijoo Search Engine Is Released in Yazd)." *Tasnim News Agency*. 04 Feb. 2015. Web. 02 June 2017. <https://www.tasnimnews.com/fa/news/1393/11/15/644626/>, and MNA. "Rahandazi-e Motor Jostejoogar-e Irani (Initiation of an Iranian Search Engine)."*Mehr News Agency*. 15 Feb. 2015. Web. 02 June 2017. <http://www.mehrnews.com/news/2495783>.

[272] Alexa. "Top Sites in Iran." *Alexa*. 02 June 2017. Web. 02 June 2017. < http://www.alexa.com/topsites/countries/IR>, and Alexa. "parsijoo.ir Traffic Statistics." *Alexa*. 02 June 2017. Web. 02 June 2017. < http://www.alexa.com/siteinfo/parsijoo.ir >, and Alexa. "yooz.ir Traffic Statistics." *Alexa*. 02 June 2017. Web. 02 June 2017. <http://www.alexa.com/siteinfo/yooz.ir>.

[273] MNA. "Nahveh-ye Hemayat Az Motorha-ye Jostejuy-e Boomi (The way the Government supports the indigenous search engines)." *Mehr News Agency*. 08 May 2015. Web. 02 June 2017. <http://www.mehrnews.com/news/2571884>.

[274] MNA. "Morurgar-e Saina Jaygozin-e Explorer Va Firefox (Saina Browser as a Substitution for Explorer and Firefox)." *Mehr News Agency*. 01 Oct. 2013. Web. 02 June 2017. <http://www.mehrnews.com/news/2140769>.

[275] Amir Rashidi, interview by author.

theft of user information, damage to their system, or use of their computer to attack others.[276] This message does not appear with Saina, suggesting its developers have intentionally or unintentionally stripped it of this functionality, leaving prospective users vulnerable to a spectrum of potential threats. The poor quality of this browser prompted many critics, including even Fars News Agency which is a conservative media outlet generally in favor of restrictive cyber policies, to question why hundreds of thousands of dollars were spent by the ICT ministry for what appears to be a slightly modified version of Firefox and why this was celebrated as a national achievement.[277]

During the presidency of Hassan Rouhani, the focus of the National Information Network has shifted back to infrastructure development. Unlike the software development that began under the Ahmadinejad administration, which is of dubious utility and may actually compromise security, infrastructure development under Rouhani has the potential to increase the speed and security and decrease the cost of domestically-hosted services.[278] As part of this approach, the administration has sought to expand infrastructure of the NIN, host more domestic websites on it, and facilitate better flow of information on it by decreasing the cost while increasing the speed of domestic traffic on this network, all while frequently emphasizing that Iranian users will remain connected to the global Internet. With the 2016 deadline of the Fifth Five Year Development Plan fast approaching, and growing pressure from Supreme Leader Ayatollah Ali Khamenei and

---

[276] LMDCICA. *Library, Museum and Document Center of the Islamic Consultative Assembly. Web. 02* June 2017. <http://www.ical.ir>.

[277] FNA. "Morurgar-e 'Irani' Copy-e Raigan-e Firefox Az Aab Dar Aamad (The 'Iranian' Browser Appears to Be a Free Replica of Firefox)." *Fars News Agency*. 24 Dec. 2013. Web. 02 June 2017. <http://www.farsnews.com/newstext.php?nn=13921003000651>.

[278] Amir Rashidi, interview by author.

principlists, the Rouhani administration redoubled its efforts by issuing a plan for the completion of the National Information Network in three phases, including Implementation (*esteghrar*), Growth (*roshd*), and Maturity (*bolugh*). The first two steps were officially announced as completed by the government in September 2016 and February 2017, respectively, with the third phase scheduled for completion in June 2017 before the end of Rouhani's first term.[279] The Rouhani administration was not able to meet its own June 2017 deadline to complete phase three and it is fair to assume this will not take place even by the end of Rouhani's second term in 2021.

The NIN project is among the largest of its kind in Iran, with more than sixty percent of the country's entire ICT budget from 2011 through 2021 (projected), or 18,409,832 million rials (829.39 million dollars) from a total of 30,598,909 million rials (1.38 billion dollars), allocated to it. In the government budget this amount is divided between three line items, including NIN infrastructure, NIN unified management, and NIN applications.[280] Table 3.1 and 3.2 demonstrate the country's entire ICT budget and NIN budget for each line item from 2011 to 2021, respectively.

Table 3.1: The Country's entire ICT Budget from 2011 to 2021 (Million Rials)

	2011-2015	2016	2017	2018-2021 (projected)	Total
The country's entire ICT budget	8,732,682	2,811,681	1,905,949	17,148,597	30,598,909

[279] ISNA. "Ejraye Phase-e Bolughe Shabakeh-ye Melli-ye Ettelaat Ta Payan Dolat (The implementation of the Maturiy Phase of the Nation Information Network by the End of the Administration)." *Iranian Students' News Agency (ISNA)*. 06 Feb. 2017. Web. 02 June 2017. <http://www.isna.ir/news/95111812481/>.

[280] MPO. "Layeh-ye Budge-ye Sal-e 1396 Kol-e Keshvar (The Country's 2017 Budget Bill)." *Management and Planning Organization of Iran*. 2016. Web. 02 June 2017. <http://www.mporg.ir/FileSystem/View/File.aspx?FileId=698c98e6-743d-49ad-8885-d23ccf2d1448>.

Table 3.2: The NIN budget from 2011 to 2021 (Million Rials)

	2011-2015	2016	2017	2018-2021 (projected)	Total
NIN infrastructure	5,828,526	1,344,530	862,349	9,416,210	17,451,615
NIN unified management	212,294	50,000	40,000	324,679	626,973
NIN applications	167,529	22,000	35,000	106,715	331,244
Total	6,208,349	1,416,530	937,349	9,847,604	18,409,832

As long as the National Information Network is viewed as an infrastructure development project that complements, rather than replaces, the global Internet, it can be seen as a net benefit to Iranian users. As noted above, these benefits can include higher speeds and lower costs when it comes to domestically-hosted services. However, depending on how the IRI decides to configure and use the NIN in the future, it can also be used as a means of coercion in at least three ways. First, the NIN would make it easier for the IRI to cut off public access to the global Internet, which provides people with a range of empowering tools, during times of domestic unrest, thereby helping it more easily confront demonstrations such as the Green Movement. This is because the NIN, which once completed will contain all of Iran's key domestic networks, could continue to function even if access to the global Internet is cut off, lowering the overall economic cost that would normally be associated with such an extreme measure.[281] The NIN can thus aid the IRI to partially alleviate the dictator's dilemma which, as discussed in the literature review, describes the trade off between maintaining greater political control versus the economic benefits conferred by cyberspace. Second, the NIN could have troubling ramifications when it comes to

[281] Amir Rashidi, interview by author.

net neutrality, the principle that Internet service providers (ISPs) should not pick winners and losers among websites and online services by modulating the speed at which users can access them. While the IRI is not capable of undermining the net neutrality principle on the global Internet, it would be able to undermine this principle within the NIN by directing traffic towards the websites and online services it likes and away from those it dislikes on this network, subtly but coercively shaping user choices.[282] The IRI would also be able to direct traffic toward websites and services on the NIN and away from foreign ones by decreasing the overall access speed to the global Internet. Finally, software development as part of the NIN, the use of which may be forced onto Iranians through legislation, could expose Iranians to a range of vulnerabilities. The software developers could deliberately build vulnerabilities and backdoors into their products, allowing the state to more freely conduct surveillance against its citizens and use information acquired by this means to more easily coerce them. These software vulnerabilities, combined with the high-level of control over hardware of the NIN by the state, give the IRI an unprecedented level of power to surveil and control the Iranian population. The greater power and intrusiveness of this system, enabled by computer technologies and the Internet, is reminiscent of the nightmarish scenarios invoked by David Burnham's Computer State or George Orwell's 1984, discussed in the literature review. Furthermore, the same vulnerabilities and backdoors used by the state can be exploited by cybercriminals to commit theft, fraud, and blackmail, among a range of illegal activities. If the IRI pursues NIN software development in this manner, Iranian users could be left at the mercy of the state and cybercriminals for the simple act of going online, especially in the absence of a strong free press and technical expert and consumer protection groups to inform them of these dangers and how to manage them.

---

[282] Amir Rashidi, interview by author.

3.2. The Comprehensive Regime of Internet Filtering

The second pillar of coercive power used by the IRI is the comprehensive regime of Internet filtering. The effort by the state to control public access to information has a long history in the Islamic Republic of Iran. The production of domestic content by the media, artists, or other entities, is controlled through censorship in order to ban production and consumption of content deemed contrary to the IRI's political ideals and cultural values.[283] The same coercive strategy has been applied to foreign content, for example content beamed in by satellite television into Iranian households. In the 1990s, when satellite television became ubiquitous in Iran, the IRI primarily focused on coercive measures to deal with it, including regular seizures of satellite dishes and systematic electronic jamming of foreign media transmissions.[284] A similar censorship effort has been undertaken by the IRI in cyberspace through the creation of a comprehensive regime of Internet filtering. According to the 2012 Internet filtering ranking published by the OpenNet Initiative, a joint research center between the University of Toronto, Harvard University and SecDev Group in Ottawa, Iran has the most restricting regime of filtering among 75 countries that were studied, including China, Pakistan, Saudi Arabia, Turkey and Syria.[285] The 2016 Freedom on the Net report by Freedom House ranked Iran among the top ten countries with the worst censorship, alongside China, Syria, Ethiopia, Uzbekistan, Cuba, Vietnam, Saudi Arabia, Bahrain,

---

[283] Hejazi, Arash. "'You Don't Deserve to Be Published'." *Logos* 22.1 (2011): 53-62.

[284] Alikhah, Fardin. "The Politics of Satellite Television in Iran." *Media, Culture and Society in Iran: Living with Globalization and the Islamic State*. Ed. Mehdi Semati. London: Routledge Taylor & Francis Group, 2010. 94-110., and Barraclough, Steven. "Satellite Television in Iran: Prohibition, Imitation and Reform." *Middle Eastern Studies* 37.3 (2001): 25-48.

[285] Rininsland, Ændrew. "Internet Censorship Listed: How Does Each Country Compare?" *The Guardian*. 16 Apr. 2012. Web. 02 June 2017. <https://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list>.

and Pakistan.[286] In this section, we explore the evolution, characteristics, and institutional basis of the comprehensive regime of Internet filtering in Iran to show how this coercive tool has been applied by the IRI to control the content Iranians can access in cyberspace.[287]

The global Internet was first introduced to Iran during the 1990s and was left relatively unregulated for three primary reasons. First, the low Internet penetration rate in Iran during this period meant that cyberspace was not a priority for censorship. Second, the technical capacity to filter content on the Internet was limited, not only in Iran but globally as well. Finally, the advent of the Internet in Iran coincided with the rise of the reformists under Mohammad Khatami, who were elected on a platform of expanding social and political freedoms. This resulted in a blossoming of publications known as the 'Press Spring' as well as greater freedom for content creators to operate online.[288] The net result was that the Internet was relatively unfiltered during much of its early existence in Iran. By the early 2000s, however, this dynamic had reversed.

As the Internet became increasingly ubiquitous in Iran, especially among the younger generation, it rose to a higher priority for the IRI as an object of censorship. Concomitantly, the technical capacity of the IRI in the area of ICTs expanded, giving it a greater capability to actually carry out censorship. The rise of this capacity was linked to greater investment in filtering technology globally, not only to combat the growing problem of cybercrime, but also increasingly the desire by

---

[286] Kelly, Sanja, Mai Truong, Adrian Shahbaz, and Madeline Earp. "Freedom on the Net 2016." *Freedom House*. Nov. 2016. Web. 02 June 2017. <https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf>.

[287] As we will see in the following sections, despite the IRI's attempts to control the content Iranians can access in cyberspace, many ordinary Iranians use circumvention tools to bypass Internet filtering and get access to content prohibited by the state.

[288] Shahidi, Hossein. "From Mission to Profession: Journalism in Iran, 1979-2004." *Iranian Studies* 39.1 (2006): 1-28.

authoritarian regimes to restrict citizen access to online content they deem as undesirable. Finally, conservatives reacted to Khatami's reforms by moving to restrict social and political reforms and rolling back many of the freedoms granted under the auspices of the Press Spring. As content creators, especially in the media, sought refuge by migrating online to avoid the censorship and political restrictions on print publications, cyberspace became a bigger target for conservatives.

One watershed moment in this process was the issuing of the "Comprehensive Policies for Computer Information Networks" by no less than Supreme Leader Ayatollah Khamenei on 3 October 1997, which laid the foundations for comprehensive filtering.[289] Article 1 of these policies declared the necessary measures should be taken to "protect the political, cultural, economic, and social security and prevent negative aspects and consequences of information networks," the first time cyberspace was explicitly tied to Iranian national security. Article 3 called for access to global information networks to be exclusively allowed through permitted institutions and organizations, the first time the question of Internet access was explicitly raised in this context.

The implementation of these policies was placed under the auspices of the Supreme Council of the Cultural Revolution (SCCR), which acts as a coordination mechanism between the branches of government in Iran on social and cultural affairs. This body includes as members the heads of the branches of government, several Cabinet ministers and other senior officials, and a handful of individuals directly appointed by the supreme leader. In December 2001 the SCCR issued the

[289] EDCS. "Siasatha-ye Kolli-ye Shabakeh-haye Ettelaresani-ye Rayaneh-i (Comprehensive Policies for Computer Information Networks)." *Expediency Discernment Council of the System*. 03 Oct. 1998. Web. 03 June 2017. <http://81.91.157.27/DocLib2/Approved%20Policies/Offered%20General%20Policies/approved%20general%20policy%20%20%2018-08-1372%20of%20%20ettelaresani.aspx.html>.

"Rules and Regulations for Computer Information Networks".[290] Article 7 of these rules and regulations, which contained 22 clauses, defined the characteristics of content that should be banned in Iranian cyberspace, which is divided into four socio-cultural, political, criminal, and audio-visual media categories in this analysis. The first category dealt with content that was deemed to oppose, criticize, satirize, or insult Islamic ideas and values and the senior Shi'a clergy, a category so broad and vague as to severely restrict the production and dissemination of such content as defined by the Islamic Republic. This category also concerned content which was deemed against the IRI's interpretation of the social and cultural values of the country and went against the lifestyle and mores promoted by the Islamic Republic. The second category related to content that was deemed to challenge the IRI, its institutions, and senior officials, including content that questioned the legitimacy and function of the IRI or promoted opposition groups in any way. The third category focused on content that facilitated crime online or in the real world through cyberspace. The final category centered on online audio-visual media portals that challenged the monopoly of the Islamic Republic of Iran Broadcasting. These categories were construed so broadly by the SCCR's rules and regulations that they constituted a comprehensive ban on a very wide range of content, a situation somewhat specific to the IRI, with the exception of the category banning content facilitating online or offline crimes, which exist almost universally around the world.

In December 2002, the SCCR took steps to implement these rules and regulations through the establishment of a committee to determine the incidents in which content should be censored in

---

[290] RCILA. "Mogharrarat Va Zavabet-e Shabakeha-ye Ettelaaresani-ye Rayaneh-i (Rules and Regulations for Computer Information Networks)." *The Research Center of the Islamic Legislative Assembly*. 03 Dec. 2001. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/100746>.

order to "protect the national and Islamic culture".[291] This committee was composed of representatives from the ministries of Intelligence and Culture and Islamic Guidance and the Islamic Republic of Iran Broadcasting, who designated specific content for censorship by the Ministry of Information and Communication Technology. By 2008, Abdol-Samad Khorramabadi, the judicial advisor of the attorney general of Iran, declared that 5 million websites had been filtered, and explained that this was necessary because "The Internet has inflicted severe damage to our society and we must plan to reduce this damage… By abusing the Internet, enemies strive to insult our religious identity."[292]

The presidency of Ahmadinejad saw significant expansions of the IRI's Internet censorship, beginning with the promulgation of the "Managing Iranian Internet Websites" statute by his Cabinet in August 2006.[293] This statute required every website opened in Iran to be registered with the Ministry of Culture and Islamic Guidance, and websites that violated the SCCR's rules and regulations on cyber content could find their permit revoked. This statute offloaded part of the burden for censorship from the IRI by creating incentives for self-censorship on the part of online content creators. This was not only due to the prospect of content censorship, but also because it would lead a content creator's permit to be revoked, restricting their ability to register websites in the future. The next major change came in 2009, with the passage of the Cybercrime

---

[291] RCILA. "Tashkil-e Committee-ye Tayin-e Masadighe-e Paygahha-ye Ettelaaresani-ye Rayaneh-i Gheyr-e Mojaz (Establishment of the Committee for Determining Incidences of Unauthorized Computer Information Networks)." *The Research Center of the Islamic Legislative Assembly*. 31 Dec. 2002. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/101083>.

[292] MNA. "Panj Million Website Dar Keshvar Filter Shodeh Ast (Five Million Websites Have Been Filtered in the Country)." *Mehr News Agency*. 18 Nov. 2008. Web. 03 June 2017. <http://www.mehrnews.com/news/784979>.

[293] IWMH. "Matn-e Kamel-e Ayinnameh-ye Samandehi-ye Paygahha-ye Interneti-ye Irani (The Full Text of the Managing Iranian Internet Websites Statute)." *The Internet Websites Managing Headquarters*. The Ministry of Culture and Islamic Guidance, 20 Aug. 2006. Web. 03 June 2017. <http://95.38.61.77/samHelp/regulation.html>.

Law by the Islamic Consultative Assembly, the Iranian parliament.[294] Article 22 of this law created the 12-member Working Group for Determining Incidences of Criminal Content in cyberspace, hereafter the Working Group (Table 3.3 lists the membership of the Working Group). This body not only superseded the SCCR committee previously tasked with determining content which should be censored but also created a much more comprehensive list of content that could be filtered.

Table 3.3: The Membership of the Working Group

1	Attorney General of the country (Chairman of the Working Group)
2	Minister of Education or a representative from the ministry
3	Minister of Communication and Information Technology or a representative from the ministry
4	Minister of Intelligence or a representative from the ministry
5	Minister of Judiciary or a representative from the ministry
6	Minister of Science, Research, and Technology or a representative from the ministry
7	Minister of Culture and Islamic Guidance or a representative from the ministry
8	Head of the Islamic Development Organization
9	Head of the Islamic Republic of Iran Broadcasting
10	Commander of Police
11	An expert selected by the Industries and Mines Committee of Parliament
12	A representative of the Judiciary and Legal Committee of Parliament

The Working Group list of banned content contains 92 clauses categorized under nine titles, vastly outnumbering the 2001 SCCR rules and regulations which had only 22 clauses.[295] The

[294] RCILA. “Ghanun-e Jarayem-e Rayaneh-yi (The Cybercrime Law)." *The Research Center of the Islamic Legislative Assembly*. 24 June 2009. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/135717>.

[295] WGDICC. "Fehrest-e Masadigh-e Mohtava-ye Mojremaneh (The List of Criminal Content Incidences)." *Working Group for Determining Incidences of Criminal Content*. Web. 03 June 2017. <http://internet.ir/crime_index.html>.

nine titles in the list are: 1) content against public decency and morality 2) content against Islamic sanctities 3) content against public security and order 4) content against public and government officials and institutions 5) content used for the commission of cybercrime 6) content used for provoking, encouraging, or inviting the commission of a crime 7) criminal content related to audio-visual and copyright right affairs 8) criminal content related to the Islamic Consultative Assembly and Assembly of Experts elections and 9) criminal content related to presidential elections. While the basic outlines of the 92 articles under these titles could be found in the 2001 SCCR rules and regulations, the Working Group list was far broader and more comprehensive in the range of content that it banned. Furthermore, while the first seven titles in the list had been dealt with to varying degrees by SCCR rules and regulations, the ban on criminal content related to the IRI's elections was completely new. This ban construes criminal content as any material that promotes a boycott of elections or decreases voter participation, calls for strikes and protests that affect elections, and distributes information deemed by the IRI to be false which impugns the integrity of the election or alleges fraud. This criminal content is also defined as including information that presents the situation of the country in a negative light or insults or libels senior officials or institutions of the country, including those tasked with overseeing and executing elections.

Interestingly, the Cybercrime Law, which led to the creation of the Working Group and its comprehensive list of banned content, was put in place in the weeks leading up to the 2009 presidential election, during which this law was applied for the very first time and on a large scale. This election spawned the Green Movement, which claimed there had been fraud in the vote counting and challenged the results by staging large nationwide demonstrations. The timing of the

new law demonstrated the sensitivity and foresight of the IRI to the potential dangers of cyberspace when it came to influencing and mobilizing people around political issues. The Green Movement, which used cyberspace as the crux of its communication and mobilization strategy, was the realization of the very dangers the IRI had contemplated when it passed the new law. In the midst of the demonstrations a vast number of websites were banned, most notably social media sites like Facebook and Twitter which had been used by the Green Movement to organize demonstrations and disseminate the movement's message. Despite the fact that many of these websites, including Facebook and Twitter, have remained banned in Iran since 2009, and accessing and publishing on them is illegal, many senior Iranian officials nonetheless use them to disseminate their message. A sample list of the most senior of these officials can be found in Table 3.4.

Table 3.4: A Sample List of the IRI Senior Officials Using Social Media Websites

Ali Khamenei (Supreme Leadr)	Facebook: @www.Khamenei.ir Twitter: @khamenei_ir
Hassan Rouhani (President)	Facebook: @rouhani.ir Twitter: @HassanRouhani Twitter: @Rouhani_ir
Javad Zarif (Minister of Foreign Affairs)	Facebook: @jzarif Twitter: @JZarif
Eshaq Jahangiri (First Vice President)	Twitter: @Eshaq_jahangiri
Mohammad Nahavandian (President's Chief of Staff)	Twitter: @Nahavandian_ir
Massoumeh Ebtekar (Head of Environmental Protection Organization)	Twitter: @ebtekarm
Mohsen Rezaee (Secretary of the Expediency Discernment Council)	Twitter: @ir_rezaee
Mohammad-Reza Aref (Leader of Reformists' Hope Fraction in Parliament)	Twitter: @ir_aref

Ali Motahari (Second Deputy of Parliament)	Twitter: @alimotahari_ir
Mahmoud Ahmadinejad (Former President)	Twitter: @Ahmadinejad1956
Ezzatollah Zarghami (Former Head of Islamic Republic of Iran Broadcasting)	Twitter: @Zarghami_ez
Gholam-Ali Haddad-Adel (Former Chairman of Parliament)	Twitter: @HaddadAdel_ir

Alongside the Working Group, another body which has come to play a decisive role in the governance structure for the filtering regime is the Supreme Council for Cyberspace (SCC). In March 2012, Iranian Supreme Leader Ayatollah Ali Khamenei ordered the creation of the SCC which is tasked with the comprehensive supervision of cyberspace on the domestic and international levels, decision-making on governing this domain, and overseeing implementation of the decisions it makes.[296] A second order by Ayatollah Khamenei in September 2015 expanded the SCC's membership and consolidated all authority for cyber policy making in its hands by dissolving all other bodies making decisions on cyberspace and transferring their power to the council.[297] The SCC is now by law the highest governing body dealing with cyber issues, incorporating some of the most senior IRI officials, with authority in this area that exceeds any one branch of government, including the executive, legislature, and judiciary (Table 3.5 lists the membership of the SCC).

---

[296] Khamenei, Ali. "Hokm-e Tashkil Va Entesaab Aza-ye Shora-ye Aali-ye Faza-ye Majazi (The Decree for the Formation and Appointment of the Members of the Supreme Council of Cyberspace)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei.* 07 Mar. 2012. Web. 03 June 2017. <http://farsi.khamenei.ir/print-content?id=19225>.

[297] Khamenei, Ali. "Hokm-e Entesaab Aza-Ye Shora-Ye Aali-Ye Faza-Ye Majazi (The Decree for the Appointment of the Members of the Supreme Council of Cyberspace)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei.* 05 Sep. 2015. Web. 03 June 2017. <http://farsi.khamenei.ir/print-content?id=30658 >.

Table 3.5: The Membership of the Supreme Council for Cyberspace (SCC)

1	President (Chairman of the SCC)
2	Chairman of Parliament
3	Head of the Judiciary
4	Head of Islamic Republic of Iran Broadcasting (IRIB)
5	Secretary of the SCC and Head of the National Center of Cyberspace
6	Attorney General of the country
7	Minister of Communication and Information Technology
8	Minister of Culture and Islamic Guidance
9	Minister of Science, Research, and Technology
10	Minister of Education
11	Minister of Defense and Armed Forces Logistics
12	Vice President for Science and Technology
13	Head of Cultural Committee in the Parliament
14	Head of Islamic Development Organisation (IDO)
15	Commander of Iranian Revolutionary Guard Corps (IRGC)
16	Commander of Police
17-24	Eight members appointed directly by the Supreme Leader

The functioning of the SCC alongside the Working Group has created a degree of structural tension within the governance structure of the filtering regime. In 2014, for example, the Working Group took the decision to place a ban on the popular WhatsApp phone and messaging application. Following the announcement of this ban Mahmoud Vaezi, minister of communication and information technology, harshly criticized the decision and declared “the subject of filtering social networks and filtering of WhatsApp was raised before the Supreme Council of Cyberspace, and the president, as the head of this council, ordered that this be stopped

and not done" in the future.[298] The Working Group's secretary bristled at this action by the SCC, declaring that "The president cannot unilaterally restrain the actions of Working Group on Detecting Criminal Content and cannot take the legal authority of decision-making about social-networks from this Working Group and transfer it to the Supreme Council of Cyberspace."[299]

In the midst of the bureaucratic turf battle between the SCC and Working Group, President Hassan Rouhani decided to take this case to the public on 20 May 2014. Speaking to an audience at the Fourth Information and Communication Technology Festival, Rouhani called for more cyber-freedoms in Iran. Invoking Marshall McLuhan's concept of the 'global village,' he remarked that "Once the discussion was that we are moving towards a 'global village', however today we are gradually moving toward a 'global family'", implying that the world had become even more interconnected since McLuhan had first coined the term.[300] Rouhani claimed that the world was now in a period in which governmental monopolization of the media landscape had come to an end:

> It seems that the era of one-sided messages has come to an end and gradually we are reaching a point where there is no place for dictatorship of the message and the era of delivering messages from one-sided megaphones, one-sided pulpits, one-sided and traditional tribunes, is over. Today any message which has a larger resonance in the world is the more powerful and impactful message.

---

[298] MNA. "Dastur-e Reis-e Jomhur Baraye Tavaghof-e Filter-e 'WhatsApp' (The President's Order to Stop the 'WhatsApp' Ban)." *Mehr News Agency*. 06 May 2014. Web. 03 June 2017. <http://www.mehrnews.com/news/2285832>.

[299] Ibid.

[300] ISNA. "Mahvareh Va Internet Amad Vali Hoviat-e Jvan-e Ma Az Dast Naraft (Satellite and the Internet Came but Our Youth's Identity Was Not Lost)." *Iranian Students' News Agency (ISNA)*. 17 May 2014. Web. 03 June 2017. <http://www.isna.ir/news/93022716896>.

In this new world, he claimed, restrictive measures towards cyberspace would no longer be effective and "the right to connect to the global information network as a civil right" had to be recognized in the country. Rouhani referenced the IRI's concern with the distribution of foreign cultural values and political ideals in Iran, which some officials label 'cultural assault', noting that simply trying to shelter Iranians from foreign content through censorship and filtering was a losing strategy:

> In culture we still hold a shield. Sometimes we hold a sword, but this is a wooden sword. We are afraid, we crawl to the corner, lest we get hit by a bullet. If a cultural assault exists – which it does – the way to combat it is not with a wooden sword. We must enter the battle with modern tools and of course not passively and with cowardice, but rather actively and bravely."[301]

The tension between the SCC and Working Group over the WhatsApp ban, and Rouhani's public statements supporting the SCC's position, appears to have resolved in favor of the latter. Today, WhatsApp is not filtered in Iran and is among the most popular messaging applications among Iranian users.

3.3. The Law and Regulation of Cyber Activities

The approach of the IRI toward shaping the production and consumption of content in Iranian cyberspace through coercion in this analysis has thus far centered on the NIN and the comprehensive regime of filtering. A third pillar of coercive power used to deter the production of, and limit access to, undesired content in cyberspace is the body of law regulating cyber activities, whose basis can be found in the preamble and articles 24 and 175 of the Constitution of the Islamic Republic. The preamble of the Constitution states that "Public communication

[301] Ibid.

instruments (radio-television) must serve the dissemination of Islamic culture in pursuit of the evolutionary course of the Islamic Revolution and in this area benefit from healthy interaction of different ideas", but "refrain from the dissemination and distribution of destructive and anti-Islamic practices."[302] This is echoed in Article 175: "The freedom of expression and dissemination of ideas in the Radio and Television of the Islamic Republic of Iran must be guaranteed in keeping with the Islamic principles and the expediencies of the country."[303] While the preamble and Article 175 refer specifically to radio and television, it shows the general principles of the IRI's media policy since its inception, which in subsequent years has been applied to cyberspace. Article 24 of the Constitution, which specifically deals with print media, states that "publications and press are free in the expression of subjects except when they are to the detriment of the fundamental principles of Islam or rights of the public. The detail is established by law."[304]

While this article left the application of constitutional principles to the media to the press law, the legislature did not pass such a law until the mid-1980s. This means that the Constitution was not merely a source of inspiration for later legislation on the media, but, in the absence of legislation, was for the first few years after the revolution a direct source of media law. According to Hossein Shahidi, based on the criteria which in large part manifested in the constitution, 175 publications were closed down only in the first three years of the Islamic Republic.[305] By using overly broad

---

[302] RCILA. "Ghanun-e Asasi-ye Jomhuri-ye Eslami (The Constitution of the Islamic Republic of Iran)." *The Research Center of the Islamic Legislative Assembly*. Web. 05 June 2017. <http://rc.majlis.ir/fa/content/iran_constitution>.

[303] Ibid.

[304] Ibid.

[305] Shahidi, Hossein. *Journalism in Iran: From Mission to Profession*. London: Routledge, 2010. p.43.

terms such as “destructive”, “anti-Islamic”, “Islamic principles and the expediencies of the country”, and “detriment of the fundamental principles of Islam” to highlight the type of content the IRI views as undesirable, the Constitution has and continues to establish a large umbrella under which a wide range of content can be banned.

The first law to address the issue of what content could and could not be conveyed by media was the Press Law, passed by the Iranian parliament in 13 March 1986 and revised in 18 April 2000. The third clause of Article 1 of the revised Press Law specifically stated that “All electronic media is covered by this law”, thereby bringing cyberspace and online content under its jurisdiction.[306] The restrictions on the production and consumption of content in the Press Law, online or otherwise, fall under Articles 5 and 6. The second clause of Article 5 gives the Supreme National Security Council (SNSC) the ability based on its discretion to restrict all media in the country from covering any topic. The SNSC is the highest governing body dealing with national security, which incorporates some of the most senior IRI officials and with authority that exceeds any single branch of government. However, the SNSC has used this authority very selectively in the past, meaning that much of the restrictions on the dissemination of content in the IRI stem from Article 6 of the Press Law and its 12 clauses.

Clause 1 bans the distribution of material deemed to be atheist, against Islamic principles, or damaging to the foundations of the Islamic Republic. Clause 2 prohibits the dissemination of content that contains obscene and religiously forbidden acts and publishing indecent pictures against public decency, while Clause 3 deals deals with content that promotes extravagance and

---

[306] RCILA. "Ghanun-e Matbuat (The Press Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 05 June 2017. <http://rc.majlis.ir/fa/law/show/91180>.

luxury. Clause 4 bans content that deals with ethnic and racial issues which create divisions within society, while Clause 5 does the same for content deemed against the security, reputation, and interests of the IRI at home and abroad. Clause 6 prohibits the revelation and dissemination of government confidential documents and orders, military secrets, and documents pertaining to closed sessions of parliament, closed trials, and judicial investigations without a legal permit to do so. Clause 7 prohibits insults against the religion of Islam and its sanctities, the supreme leader, and senior Islamic jurists. Clause 8 outlaws libel not only against public officials, institutions, and organizations, but any citizen of the country, as well as insults against any legal and real persons who possess religious sanctity, even through the dissemination of pictures and caricatures. Clause 9 outlaws committing plagiarism and quoting domestic or abroad deviant media outlets, parties, and groups that are against Islam in such a manner as to propagate their ideas. Clause 10 proscribes exploitation of individuals through images or other content, degrading and insulting the female gender, and promoting ostentatious displays and luxury that are illegitimate and illegal. Finally, Clause 11 enjoins the circulation of baseless rumors or distortion of the content of others, while Clause 12 mirrors this for content which is against the Constitution. As these clauses demonstrate, the Press Law did not fulfill the promise of Article 24 of the Constitution to flesh out the details of its ban on content deemed to be "detriment of the fundamental principles of Islam or rights of the public". Instead, its 12 clauses contained restrictions on content that were just as vague and unclear, creating an umbrella under which a wide range of content could be banned.

Every media organization operating on- or offline in the IRI needs a permit, and the Press Law determines both who can acquire a permit and the consequences when the conditions of a permit

are violated. According to the Press Law individuals who are members and supporters of anti-revolutionary or illegal groups, have been condemned in court for working against the revolution and national security, and who are active or engaged in propaganda against the Islamic Republic cannot acquire a permit nor hold any media job. In practice, these individuals do not only include dissenters who are firmly outside of the political system, but also many former consummate insiders and senior officials of the IRI who ran afoul of the system and have been condemned in court because of their political activities, including leading figures of the Reform and Green movements.

If an individual actually manages to acquire a permit, they must remain in good standing by complying with the Press Law. Violations of this will result in two months to two years in prison or up to 74 lashes, and repeated violations can result in the permanent revocation of their permit alongside increased punishment. In the case of content that is deemed as an action against national security (Clause 5), reveals military secrets (Clause 6), or constitutes an insult against Islam and its sanctities (Clause 7), there is additional punishment under Iranian law. Finally, content deemed as an insult against the supreme leader and senior Islamic jurists (Clause 7) carries further punishment for the writer of the article under the criminal law and revocation of the press permit of the publication. These and other punishments meted out under Iranian law are elaborated upon below.

The Press Law deals with big media, which made up of professional organizations that require a permit to legally operate. However, the increasing access of ordinary Iranians to cyberspace has generated an explosion of online content produced by them through a variety of outlets, most

notably weblogs, social media networks, and messaging applications such as Facebook, Twitter, Instagram, and Telegram. Both the nature of this content, which does not require big media to produce, as well as its sheer volume, have created a challenge for the IRI, which it has attempted to manage through a variety of other laws alongside the Press Law. Beyond the latter, this analysis has identified nine other laws that cover and regulate a wide range of activities in cyberspace.[307] Appendix 1 provides a sample list of these activities and the specific punishments they entail, dividing them into four socio-cultural, political, security, and cyber criminal categories.

The socio-cultural category deals with online activities that insult the religion of Islam and its sanctities. Terms such as "insult" and "sanctities" are vague and have not been defined in a detailed and accessible manner that would allow ordinary Iranians to easily navigate their way around these laws. This allows for judges to interpret laws falling in this category quite broadly, a fact compounded by the reality that sentences on these crimes can be as serious as the death penalty. Sina Dehghan, for example, at the time of writing has been sentenced to death on the grounds that he insulted the Prophet Mohammad for the contents of messages he wrote over the Line social media application.[308] Broad interpretations of these terms have a precedence in the history of the IRI. For example, in 15 June 1981, the National Front publicly argued against the death penalty, sanctioned by Islamic law, on the grounds that it was unjust and inhumane. This resulted in the decision by the Ayatollah Ruhollah Khomeini to declare them apostates on the

---

[307] The laws identified in this analysis include the: 1) Islamic Penal Law 2) Cybercrime Law 3) Law on Electronic Commerce 4) Law to Protect the Copyrights of Software Developers 5) Penal Law on the Leaking and Publishing of Secret and Confidential Governmental Material 6) Penal Law on Smuggling and Illegal Ownership of Arms and Ammunition 7) Penal Law on the Illegal Activity in the Domain of Audio-Video Materials 8) Islamic Consultative Assembly Elections Law, and 9) Presidential Elections Law.

[308] CHRI. "Young Man Facing Death for Insulting Islam Online Tricked into Signing Confession."*Center for Human Rights in Iran*. 24 Mar. 2017. Web. 05 June 2017. <https://www.iranhumanrights.org/2017/03/young-man-facing-death-for-insulting-islam-online-tricked-into-signing-confession/>.

grounds they had insulted Islamic sanctities, a charge which itself can carry the death penalty. A broad definition of Islamic sanctities that includes Islamic Law could preclude the ability of people to criticize a major part of Iranian law.[309]

The socio-cultural category also concerns activities deemed to be against the social and cultural values, lifestyle, and mores promoted by the Islamic Republic. Again, this category contains terms such as "obscenity" and "public decency" that are vague and leave ample latitude for judges to interpret them. Often times crimes in the socio-cultural category go beyond the public realm into Iranians' private spaces, even covering personal photography, artistic endeavors, and fashion, among other things. Laws in this category can serve as a sword of Damocles hanging over people's heads for what appear to be innocuous personal activities, as for instance illustrated by the case of Saeed Malekpour: a Canadian permanent resident of Iranian origin, who was arrested in Iran while visiting his ailing father on the grounds that a computer software he had developed had been used in a pornography website. Regardless of Malekpour's knowing involvement in this application of his software, he received the death penalty, a sentence later commuted to life in prison.[310]

The political category includes online activities that challenge the IRI, its institutions, senior officials, and legitimacy and function. The laws under the political category include overly broad terms such as "insulting and degrading", "spreading falsehoods and disturbing the public opinion", and "spreading propaganda" against the IRI, which create a large umbrella under

---

[309] Khomeini, Ruhollah. "Sahifeh-ye Imam. Vol. 14." *The Institute for Compilation and Publication of Imam Khomeini's Works*. Web. 05 June 2017. <http://statics.ml.imam-khomeini.ir/en/File/NewsAttachment/2014/1708-Sahifeh-ye%20Imam-Vol%2014.pdf>.

[310] Kamali Dehghan, Saeed. "Iranian Web Programmer Faces Execution on Porn Charges." *The Guardian*. 09 Feb. 2011. Web. 05 June 2017. <https://www.theguardian.com/world/2011/feb/09/iranian-death-sentence-pornography>.

which a wide range of publication and distribution activities in cyberspace become punishable. Under this umbrella, virtually any criticism of state policies can breach the law, opening the accused to charges that they have worked against national security, as happened in the tragic case of blogger Sattar Beheshti, discussed in greater detail later in this section.[311] The security category focuses on actions against Iranian national security, which includes a wide range of activities such as publishing content that involves a bomb threat, inciting people to violence, provoking military forces to dereliction of duty, desertion, or surrender, and selling, advertising, and distributing any type of arms and ammunition. This category also includes leaking and publishing secret and confidential governmental material. The security category, and the harsh punishment it includes, are not unique to the IRI, but are features of states around the world. However, when it comes to leaking and publishing secret and confidential governmental material, Iranian law is harsher than analogous laws in some other countries. This is because in Iran those who publish this material, for instance journalists, are punished just as harshly as leakers.

Finally, the cyber criminal category pertains to criminal activities in cyberspace or those facilitated by cyberspace in the real world. This includes digital fraud and forgery, infringing on consumer rights, unauthorized access to personal data, and illegally accessing to use or leak trade secrets. This category also includes infringing on intellectual property rights, namely copyrights and trademarks. The cyber criminal category is not unique to the IRI, but like the security category, features in the laws of states around the world. In the case of the IRI, however, it can be argued that when it comes to infringement of intellectual property rights, the punishments do not

---

311 Kamali Dehghan, Saeed. "Iran Accused of Torturing Blogger to Death." *The Guardian*. 08 Nov. 2012. Web. 05 June 2017. <https://www.theguardian.com/world/2012/nov/08/iran-accused-torturing-blogger-death>.

go far enough to adequately act as a deterrent to the rampant violation of these laws that takes place in Iran. Of the four categories outlined above, the first two, composed of the socio-cultural, and political categories, possess a high degree of restrictiveness due to the breadth of the range of activity they cover and severeness of their punishment. The last two, composed of the security and cybercrime categories, in contrast, can be found in the body of cyber laws in most countries around the world and can be seen as addressing justifiable concerns.

The laws dealing with cyberspace, divided into four categories and discussed at length above, are implemented in the IRI by two law enforcement bodies. The Police for the Sphere of the Production and Exchange of Information, usually referred to by its acronym FATA in Persian and labelled as the Cyber Police hereafter, was established on 23 January 2011 under the auspices of the Iranian Police. Then chief of Police, Esmail Ahmadi-Moghaddam explained that the Cyber Police had been formed as a response to the assassination of Iranian nuclear scientists, allegedly by Israel, which he asserted had been planned and coordinated in large part in cyberspace.[312] While the use of cyberspace for conducting terrorist operations was cited as a motivation for the creation of the Cyber Police, the rise of the Green Movement demonstrations just a year and a half earlier as well as the rising challenge posed by cybercrime may have also been motivating factors. The responsibilities and missions of the Iranian Cyber Police include the "creation of security and decreasing of threats for scientific, economic, social activities" and "protecting and defending religious and national identity" in cyberspace, and "safeguarding and overseeing" cyberspace in order to prevent it from becoming a "breeding ground" for "illegal activities and

[312] MNA. "Enfejarha Va Havades-e Akhir Az Tarigh Fazaye Majazi Modiriat Mishavad (Recent Explosions and Incidences are Managed through Cyberspace)." *Mehr News Agency*. 23 Jan. 2011. Web. 05 June 2017. <http://www.mehrnews.com/news/1238040>.

thereby "avoid assault against the ideas and norms of society".[313] According to a report published by the Cyber Police, 70 percent of the crime in Iran takes place in cyberspace, which indicates that much of the country's crime is either conducted directly within cyberspace or facilitated by it offline. Of all cybercrime, 52 percent is unauthorized financial withdrawals, 34 percent libel, blackmail, and harassment, and 14 percent is made up of other crimes.[314]

Among the four categories punishable under the Iranian laws highlighted above, much of the activity of the Cyber Police appears to be focused on cybercrime and security, while political, and socio-cultural issues have received far less attention, although some incidents show the involvement of this body in these areas as well. The tragic case of Sattar Beheshti, a working-class blogger on social and political issues from Tehran, is just one example of such incidents. Beheshti was arrested on 30 October 2012 on charges of actions against national security as a result of publishing content criticizing the government on social media, and died under interrogation while in the custody of the Cyber Police four days later. As a result of the public and international outcry over this incident, the head of the Cyber Police in Tehran was dismissed, although it is unclear if the true perpetrators of Beheshti's death have been held to account.[315]

The Islamic Revolutionary Guard Corps, as the pre-eminent security institution in the IRI, has also played an important law enforcement role in the cyber domain through its Center for the Investigation of Organized Crimes in cyberspace (CIOC), created in 2007. The responsibilities

---

[313] CP. "Sharh-e Vazayef Va Mamuriat-ha (Overview of Missions and Responsibilities)." *The Cyber Police*. Web. 05 June 2017. <http://www.cyberpolice.ir/page/127>.

[314] Jafari, Mehrdad. "Hameh Ba Ham Baraye Amniat Va Aramesh (All together for Security and Tranquillity)." *The Cyber Police*. Web. 05 June 2017. <http://www.cyberpolice.ir/sites/default/files/fata.pdf>.

[315] Kamali Dehghan, Saeed. "Iran Accused of Torturing Blogger to Death." *The Guardian*. 08 Nov. 2012. Web. 05 June 2017. <https://www.theguardian.com/world/2012/nov/08/iran-accused-torturing-blogger-death>.

and mission of this organization include confronting the "widespread effort of the enemy to destroy the cultural structure of society", the activities of "opposition groups", "the change of people's lifestyle", cyber espionage and sabotage, and unauthorized circumvention of the filtering regime.[316] Among the four categories punishable under the Iranian laws highlighted above, the IRGC CIOC emphasizes the political, and socio-cultural categories, as demonstrated by the operations it has conducted. In Operations "Those Who Lead Astray" I-V in 2009, this body arrested website administrators and shut down websites which created and distributed content it deemed to be of a sexual nature in Persian, insulted Islamic sanctities, promoted the boycott of elections and distributed atheistic and anti-religious books and the news of anti-revolutionary groups. In Operation Fox Eye in 2012, the IRGC CIOC rolled up a network of individuals which it believed to be linked to BBC Persian by arresting 17 individuals. In Operation Spider I in 2012, it took actions similar to those in Operations "Those Who Lead Astray" I-V, but with a focus on Facebook, arresting page administrators and closing 300 pages. In Operation Spider II in 2016, the IRGC CIOC targeted Instagram page administrators and pages linked with the fashion industry, including models, beauty salons, photo studios, fashion studios, and design schools. In total 170 individuals linked with over 300 pages were targeted, including 58 models, 51 heads of fashion studios, 59 hair stylists and photographers, and two heads of design schools. Overall, 29 of these individuals had their businesses closed and 8 of them were arrested.[317]

---

316 Gerdab. "Farmandehi-ye Amniat-e Cyberi-ye Sepah-e Pasdaran-e Enghelab-e Eslami (The Cyber Security Command of the Islamic Revolutionary Guard Corps)."*Gerdab*. The IRGC Cyber Security Command, Web. 05 June 2017. <http://www.gerdab.ir/fa/about>.

317 Gerdab. "Tarikhcheh-ye Parvandehha-ye Rasanehi-ye Shodeh-ye Gerdab (The Record of Gerdab's Publicized Files)." *Gerdab*. The IRGC Cyber Security Command, 15 Sept. 2015. Web. 05 June 2017. <http://www.gerdab.ir/fa/news/15588>.

The activities of the IRGC CIOC have not only affected individuals working in traditionally tightly controlled or prohibited sectors in Iran, but have even found their way into Iranian mainstream politics. In March 2017, 12 administrators of six Telegram channels with large followings associated with the reformist political current were targeted and either had the pages closed, archives erased, or stopped activities altogether. This caused an uproar among some senior IRI officials, including the Rouhani administration spokesman Mohammad Bagher Nobakht and Intelligence Minister Mahmoud Alavi, among others.[318] Having happened in the lead up to the 2017 Iranian presidential election, the targeting of Telegram channels had potentially important political implications, given that Telegram is one of the primary means through which reformists could mobilize their large body of supporters to vote for the reelection of their favored candidate, incumbent President Rouhani.

3.4. Iran and the Exercise of Coercive Power at the Global Level

The National Information Network, comprehensive regime of filtering, and restrictive body of law regulating cyber activities constitute the foundation of coercive measures used by the IRI towards Iranian society at the domestic level. This section analyzes the IRI's defensive and offensive measures to exercise coercive power against its rivals at the global level. The IRI's need to take defensive measures has been shaped by the cyber attacks conducted against it by rival state actors since 2009, making it among the first victims of coercive action in cyberspace by one state against another. Prior to this, the only comparable cases to the attacks on Iran were Russian cyber attacks against Estonia in 2007 and Georgia in 2008, where government, bank and

[318] Karimi, Arash. "Rouhani Government Criticizes IRGC Arrests of Journalists." *Al-Monitor*. 06 Apr. 2017. Web. 05 June 2017. <http://www.al-monitor.com/pulse/originals/2017/04/iran-elections-telegram-journalists-channels-arrested.html>.

newspaper websites were disrupted, and Kyrgyzstan in 2009, where attacks on Internet Service Providers resulted in a major loss of Internet functionality throughout the country.[319] However, one of the first major cases of an offensive cyber operation by state actors was the use of the Stuxnet worm to target Iranian nuclear facilities in Fall 2009, allegedly by the United States and Israel.[320] Stuxnet was designed to alter the operation of Siemens Simatic process logic controller computers used in Iranian uranium enrichment infrastructure.[321] By drastically changing the speed at which uranium enrichment centrifuges operated at uranium enrichment center at Natanz, Stuxnet destroyed up to 1000 centrifuges, or approximately 10 percent of the total supply, thereby slowing the progress of the Iranian nuclear program at a sensitive moment in the nuclear dispute between the IRI and its rivals.[322] Stuxnet was followed by another attacked called 'Duqu' against the Iranian nuclear program in September 2011. Symantec, an American security software company, analyzed Duqu and confirmed that it is "nearly identical to Stuxnet, but with a completely different purpose".[323] According to Symantec, the purpose of Duqu, unlike its destructive predecessor Stuxnet, was to gather information on Iranian industrial infrastructure for planning future attacks. Although it is not clear who was behind the operation, Symantec

---

[319] Kozlowski, Andrzej. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan." *European Scientific Journal* 3.Special Edition (2014): 237-45.

[320] Nakashima, Ellen, and Joby Warrick. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." *The Washington Post*. 02 June 2012. Web. 05 June 2017. <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.0f7912d38fe6>.

[321] Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier." *Symantec*. Feb. 2011. Web. 05 June 2017. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

[322] Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report." *Institute for Science and International Security*. 15 Feb. 2011. Web. 05 June 2017. <http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf>.

[323] Symantec. "W32.Duqu: The Precursor to the next Stuxnet." *Symantec*. 23 Nov. 2011. Web. 05 June 2017. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>. p.1.

believes that Duqu is created by the Stuxnet authors or those that have access to the Stuxnet source code.

These attacks made the IRI aware of the vulnerability of the country's industrial and ICT infrastructure to a wide range of cyber sabotage and espionage operations. As a result of the damage cause by Stuxnet and Duqu, the IRI's leadership took defensive measures to protect this infrastructure against future attacks. Following the Duqu attack, the Cyber Defense Headquarters (CDH) was formed on 30 October 2011 under the auspices of the General Staff of the Armed Forces of the Islamic Republic of Iran.[324] According to Article 5 of the Cyber Defense Strategic Document, this body is the highest authority in Iran dealing with cyber defense, with the mission to "immunize and stabilize the cyber systems of the country by overseeing, analyzing and identifying threats" and "discovering, managing, and controlling vulnerabilities".[325] The CDH is also responsible for issuing warnings on cyber threats, cyber defense institution building and education, and compiling and publishing cyber defense measures, including its principles, regulations, requirements, and considerations. Finally, it is responsible for commanding cyber defense operations and legal defense against external cyber threats and attacks on the international stage.[326]

Following its formation, the CDH rapidly implemented defensive measures over Iranian cyberspace, but the country soon experienced another major cyber attack as a result of the

---

[324] MNA. "Farman-e Tashkil-e Gharargah-e Cyberi Dar Keshvar Eblagh Shod (The Decree for the Formation of the Cyber Defense Headquarters in the Country Was Issued)." *Mehr News Agency*. 30 Oct. 2011. Web. 05 June 2017. <http://www.mehrnews.com/news/1447810>.

[325] ITDMC. "Sanad-e Rahbori-ye Padafand-e Cyberi-ye Keshvar (The Country's Cyber Defense Strategic Document)." *Information Technology and Digital Media Center*. Ministry of Culture and Islamic Guidance, 11 June 2015. Web. 05 June 2017. <http://www.saramad.ir/Content/media/filepool3/2015/11/2946.pdf>. p.4.

[326] Ibid.

'Flame' malware in 2012, which targeted Ministry of Oil computers.[327] Like Duqu, this malware appears to have been written purely for espionage in order to gather information on industrial infrastructure for planning future attacks. Flame impacted key elements of the oil sector's ICT infrastructure, including the oil ministry and National Iranian Oil Company (NIOC) in Tehran and other locations, as well as oil facilities at Siri, Lavan, Kish, Khark, Gheshm, and Behregan, which were cut off from the oil ministry's ICT systems.[328] It is unclear whether this network blackout was a direct result of the Flame attack or part of the preventative measures taken by the oil ministry to prevent further damage. Attacks against petroleum infrastructure are particularly concerning for the IRI given the reliance of the Iranian economy on oil exports, with production stoppages having significant negative ramifications for the economy. Although independent experts have not been able to confirm who was behind the attack, the Washington Post claimed on 19 June 2012 that Flame was a joint US-Israeli operation to collect intelligence in preparation for further cyber attacks to inflict economic pain on the IRI in order to affect its nuclear decision-making.[329] This case shows how cyber espionage operations can cause significant economic damage by not only stealing valuable information, but also forcing victims to shut off their own network to prevent the further spread of malware, thereby wreaking additional damage. Regardless, the Flame malware appears to have been the last major cyber attack on Iran, which

---

[327] Symantec. "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East." *Symantec*. 28 May 2012. Web. 05 June 2017. <https://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east>.

[328] MNA. "Tashkile Setad-e Bohran-e Cyberi Dar Vezarat-e Naft (Formation of the Cyber Crisis Headquarters in the Oil Ministry)." *Mehr News Agency*. 23 Apr. 2012. Web. 05 June 2017. <http://www.mehrnews.com/news/1584142>.

[329] Nakashima, Ellen, Greg Miller, and Julie Tate. "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say." *The Washington Post*. 19 June 2012. Web. 05 June 2017. <https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.e2052df3ea63>.

may be an indication that the Cyber Defense Headquarters has largely been successful in its mission to secure Iranian cyberspace.[330] However, a second explanation may be that the fall off of attacks is a result of the decreased tensions between Iran and its rivals following resolution of the nuclear dispute in 2015, given that the preponderance of cyber operations against the country up to this point were in one way or another linked to the nuclear issue.

When it comes to cyberspace however, defensive measures, by themselves, are not sufficient to deter rivals who want to use this domain to carry out attacks. Offensive measures are also necessary to demonstrate to rivals the capability to retaliate in case of an attack and thereby establish a deterrence relationship.[331] With cyberspace, as with other domains, a good offense is often also a good defense. To this end, the IRI has developed an offensive capability in the form of a designated unit to conduct such operations. The creation of just such capability was announced by Brigadier General Gholam-Reza Jalali, head of Iran's Passive Defense Organization, on 06 March 2011. Jalali stated that Iran would create a Cyber Offensive Headquarters (COH), an organization that complements the Cyber Defense Headquarters.[332] Jalali openly called on hackers who wanted to serve the interests of the Islamic Republic to join the ranks of this organization. In a later statement on 20 February 2012, he announced that the IRI would build the first cyber army, declaring that the "U.S. is downsizing its army for bigger

---

[330] Amir Rashidi, interview by author.

[331] Shaheen, Salma. "Offense–Defense Balance in Cyber Warfare." *Cyberspace and International Relations Theory, Prospects and Challenges*. Ed. Jan-Frederik Kremer and Benedikt Müller. Berlin: Springer Berlin, 2016. 77-94.

[332] BTA. "Gharargah-e Jang-e Cyberi Rahandazi Mishavad (The Cyber Warfare Headquarters Will Be Stablished)." *Bultan News Agency*. 06 Mar. 2011. Web. 05 June 2017. <http://www.bultannews.com/fa/news/41662>.

cyber defense infrastructure. So countries like Iran also have to set up and upgrade their cyber defense headquarters and even [build] a cyber army".[333]

The initial context in which the COH and Iranian Cyber Army (ICA) were initially shaped and carried out operations was that of Iranian domestic politics and the Green Movement. The first category of offensive cyber operations were primarily against domestic and foreign news websites and Internet giants which supported or were seen by the IRI as supporting the Green Movement in one form or another. Cyber attacks disrupted pro-Green Movements websites Moj-e Sabz-e Azadi (16 December 2009), Jaras (12 February 2010), Tahavol-e Sabz (12 February 2010) and Kaleme (12 February 2010),[334] the latter being officially linked with Green Movement leader Mir-Hossein Mousavi, undermining the ability of the movement's leadership to issue official statements and communicate with their base. Cyber attacks were also carried out against foreign-funded and -based Persian language news websites that communicated the daily drama of the Green Movement to the world, including the Netherlands-based Radio Zamaneh (29 January 2010)[335] and U.S.-based Voice of America, which is linked with the American government (21 February 2011).[336] Finally, cyber operations which caused disruptions were also carried out against Internet giants such as Twitter (18 December 2009)[337] and Baidu (12 January

---

[333] Press TV. "'Iran Set to Build First Cyber Army'." *Press TV*. 20 Feb. 2012. Web. 05 May 2017. <https://web.archive.org/web/20120621015437/http://www.presstv.ir/detail/227739.html>.

[334] BBC. "Hamleh-ye Interneti-ye Tazeh Be Site-haye Interneti-ye Motarezan-e Irani (New Cyber Attack Against the Iranian Protestors' Websites)." *BBC Persian*. The British Broadcasting Corporation (BBC), 12 Feb. 2010. Web. 05 June 2017. <http://www.bbc.com/persian/iran/2010/02/100212_l06_jaras_kalameh_hacking.shtml>.

[335] Kronenburg, Ruth, and Farid Haerinejad. "Radio Zamaneh Hacked by Iranian Cyber Army."*Radio Zamaneh*. 01 Feb. 2010. Web. 05 June 2017. <http://www.zamaaneh.com/enzam/2010/02/radio-zamaneh-hacked-by-i.html>.

[336] Ide, William. "Iranian Hackers Attack VOA Internet Sites." *Voice Of America (VOA)*. 21 Feb. 2011. Web. 05 June 2017. <https://www.voanews.com/a/iranian-hackers-attack-voa-internet-sites-116678844/172741.html>.

[337] Johnson, Bobbie. "Twitter 'hijacked by Iranian Hackers'." *The Guardian*. 18 Dec. 2009. Web. 05 June 2017. <https://www.theguardian.com/technology/2009/dec/18/twitter-hijacked>.

2010).[338] The social media website Twitter played an important role in the Green Movement by acting as a tool of mass self-communication for Iranian users in the movement, and even delayed website maintenance so as not to impede the movement or these users. Somewhat more puzzlingly, the Chinese search engine Baidu was targeted, likely because of the support shown by Chinese Internet users for the Green Movement through the hashtag #CN4Iran.

These attacks indicated the range of Iranian cyber offensive capabilities, which were able to disrupt everything from less secure websites, to more secure foreign-funded and -based news websites, to giants like Twitter and Baidu which have robust security. The ICA made its presence known by defacing websites with its logo and slogans, which sent a clear message to victims about the rationale behind why they were targeted, specifically their role in facilitating support for the Green Movement in one way or another. This message was compounded by statements from the IRI's mainstream media and even senior Iranian military officials who boasted of the attack, including Mojtaba Zolnoor, deputy representative of the supreme leader to the IRGC, who told the 9 Dey weekly newspaper on 26 April 2011 that the ICA had a "promising and phenomenal" record of hacking and shutting down many websites deemed by the IRI to be associated with the enemy.[339]

The second category of the IRI's offensive cyber operations possessed a number characteristics that distinguish it from the first category, namely a higher level of technical sophistication that went beyond defacement, no direct linkage to Iranian domestic politics and the Green

---

[338] Branigan, Tania. "'Iranian' Hackers Paralyse Chinese Search Engine Baidu." *The Guardian*. 12 Jan. 2010. Web. 05 June 2017. <https://www.theguardian.com/technology/2010/jan/12/iranian-hackers-chinese-search-engine>.

[339] Dey 9th. "Ghoveh-ye Ghazaieh Dar Barkhord Ba Saran-e Fetneh Barkhord-e Amali Konad (The Judiciary Shall Take Concrete Measures to Confront the Sedition Leaders)." *Dey 9th Weekly Newspaper*. 26 Apr. 2011. Web. 05 June 2017. <https://web.archive.org/web/20111101184327/http://www.9day.ir:80/article/274>.

Movement, and no acknowledgement of responsibility. One of the earliest and most significant offensive cyber operations in this second category targeted the U.S.-based Comodo (March 2011)[340] and Netherlands-based DigiNotar (August 2011)[341], two ICT companies that created Secure Sockets Layer (SSL) certificates used by a wide variety of clients, including leading tech firms with a large number of users around the world such as Google. Secure Sockets Layer certificates safeguard the stored and transmitted personal data of users, including sensitive material like passwords and financial information. By gaining access to SSL certificates, a hacking entity can bypass security measures on user data and conduct surveillance or other cyber operations. In the case of DigiNotar nearly 300,000 SSL certificates were stolen, many of these for Iranian users of Google, prompting the tech giant to announce that "The people affected were primarily located in Iran" and warn these users of the risk of surveillance by the hacking entity.[342] According to statements by the Dutch government and reports by the independent technical community, this attack was carried out by the IRI with the primary goal of gaining the ability to conduct surveillance against Iranian users, rather than financial gain, sabotage, or other objectives.[343] Although the main goal appears to have been surveillance of Iranian users, the fallout went beyond this to include the bankruptcy of DigiNotar. According to the Dutch

---

[340] Comodo. "Comodo SSL Affiliate The Recent RA Compromise." *Comodo Blog*. Comodo, 23 Mar. 2011. Web. 05 June 2017. <https://blog.comodo.com/other/the-recent-ra-compromise/>.

[341] Meulen, Nicole Van Der. "DigiNotar: Dissecting the First Dutch Digital Disaster." *Journal of Strategic Security* 6.2 (2013): 46-58.

[342] Google. "An Update on Attempted Man-in-the-middle Attacks." *Google Online Security Blog*. Google, 29 Aug. 2011. Web. 05 June 2017. <https://security.googleblog.com/2011/08/update-on-attempted-man-in-middle.html>.

[343] GN. "Interim Report: DigiNotar Certificate Authority Breach "Operation Black Tulip"."*Government of the Netherlands*. 05 Sept. 2011. Web. 05 June 2017. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf>, and GN. "Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach."*Government of the Netherlands*. 13 August. 2012. Web. 05 June 2017. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf>.

Ministry of Justice, the SSL certificates stolen in this breach would allow Iran to breach security protocols for tech giants such as Yahoo, Facebook, Microsoft, Skype, AOL, Mozilla, TorProject, and WordPress, and intelligence agencies, including the CIA, Israel's Mossad and Britain's MI6.[344] The complexity and skill with which these attacks were orchestrated led Google Executive Chairman Eric Schmidt to tell CNN that: “Iranians are unusually talented in cyber warfare for some reason we don’t fully understand.”[345]

Another major offensive cyber operation by Iran took place on 15 August 2012 against the computer network of Saudi Aramco, the world's largest oil and gas company, which was struck by a computer virus dubbed ‘Shamoon’ and infected 30000 computers in its network.[346] Shamoon’s main role was to delete data from Aramco computers, thereby disrupting the company’s activity by making the company’s website experience significant periods of downtime and deleting some sensitive files related to drilling and production data. This imposed a major economic cost, although it did not result in an oil spill, explosion, or other major physical damage to the company’s infrastructure.[347] The Anti-Oppression hacker group released a statement taking responsibility for the attack immediately following the operation, which has been reproduced below:

---

[344] NYT. "Hacking in the Netherlands Took Aim at Internet Giants." *The New York Times*. 05 Sept. 2011. Web. 05 June 2017. <http://www.nytimes.com/2011/09/06/technology/hacking-in-the-netherlands-broadens-in-scope.html>.

[345] CNN. "Google's Eric Schmidt on Protecting America's Tech Secrets." *CNN*. 13 Dec. 2011. Web. 05 June 2017. <http://outfront.blogs.cnn.com/2011/12/13/googles-eric-schmidt-on-protecting-americas-tech-secrets/>.

[346] Nakashima, Ellen. "Cyberattack on Mideast Energy Firms Was Biggest Yet, Panetta Says."*The Washington Post*. 11 Oct. 2012. Web. 05 June 2017. <https://www.washingtonpost.com/world/national-security/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html?>.

[347] Bronk, Christopher, and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco." *Survival* 55.2 (2013): 81-96.

1. We, behalf [sic] of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.
2. One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
3. In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.
4. This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.
5. Cutting Sword of Justice [348]

Key details in the statement by the attackers, including the time of the attack (11:08 AM) and number of computes targeted (30,000), as well as their IP addresses published separately by the hackers later on, were confirmed by ARAMCO. The technical expert community cited Iran as the source of the attack and through analysis of Shamoon found that its source-code appeared similar to Flame, the malware discovered conducting espionage in the Iranian oil ministry's computer networks that same year.[349] This is illustrative of the IRI's high level of expertise and capabilities in analysing sophisticated malware such as Flame and re-engineering them for its own ends and uses. The Shamoon attack came in the context of heightened geopolitical tension between Iran and Saudi

[348] Pastebin. "Untitled." *Pastebin*. 15 Aug. 2012. Web. 05 June 2017. <https://pastebin.com/HqAgaQRj>.

[349] Bronk, Christopher, and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco." *Survival* 55.2 (2013): 81-96.

Arabia, and at a time when Iranian oil exports decreased because of international sanctions, with the resulting gap in the international oil supply filled by Saudi ARAMCO.

The last example is the series of cyber attacks between late 2011 and mid-2013 came to light when the United States Attorney for the Southern District of New York unsealed an indictment on 24 March 2016 to charge seven Iranian hackers affiliated with two government-sponsored hacking groups, named ITSecTeam and Mersad Company.[350] According to court documents the hackers conducted a coordinated campaign of distributed denial of service (DDoS) attacks against 46 major companies, primarily in the U.S. financial sector between December 2011 and September 2012.[351] These attacks disabled the websites of the targeted banks, prevented customers from accessing their online accounts, and altogether cost the banks tens of millions of dollars in remediation costs as they worked to neutralize the attacks on their servers and mitigate the fallout. These attacks disrupted the business operations of the targeted banks and interfered with their customers' ability to do online banking while the attacks were underway, but did not affect customer account data or result in its theft. One of the hackers was also charged with unauthorized access to the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, in Rye, New York, between August 28, 2013, and September 18, 2013. The indictment highlights that the hacker obtained critical information about the dam's operation,

---

[350] DOJ. "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities." *The United States Department of Justice*. 24 Mar. 2016. Web. 05 June 2017. <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated>.

[351] DOJ. "United States of America Vs Ahmad Fathi; Hamid Firoozi; Amin Shokohi; Sadegh Ahmadzadegan, a/k/a Nitr0jen26; Omid Ghaffarinia, a/k/a Plus; Sina Keissar; And Nader Saedi, a/k/a Turk Server." *The United States Department of Justice.* 24 Mar. 2016. Web. 05 June 2017. <https://www.justice.gov/usao-sdny/file/835061/download>.

including the sluice gate that controls water levels and flow rates. The hacker's access to this information enabled him to remotely operate and manipulate the sluice gate, although at the time of this attack the gate was disconnected for maintenance. According to the court documents, two of the hackers involved in this series of attacks had also claimed responsibility for previous major attacks, including intrusion into the National Aeronautics and Space Administration (NASA) servers in February 2012 and many other servers in the United States, United Kingdom and Israel. As a result of the charges, these seven Iranian hackers are now under International Police (Interpol) red notices that would result in their arrest should they choose to travel outside of Iran. [352]

Since these three major offensive cyber operations between 2011 and 2013, there have not been major cyber attacks that can be attributed to the IRI with a high level of confidence. There are at least two, not mutually exclusive, explanations why this may be the case. One compelling explanation may be that the election of Hassan Rouhani in 2013 and signing of the Joint Comprehensive Plan of Action (JCPOA) in 2015 decreased overall tensions between the IRI and its adversaries and, therefore, major cyberattacks as well. A second explanation is that these major cyber attacks by the IRI demonstrated its capabilities as a cyber-power, established a level of deterrence vis-a-vis its adversaries, and created an equilibrium whereby further major attacks by either side could lead to unwanted escalation in tension and conflict.

---

[352] FBI. "Iranians Charged with Hacking U.S. Financial Sector." *Federal Bureau of Investigation (FBI)*. 24 Mar. 2016. Web. 05 June 2017. <https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector>.

Conclusion

This chapter examined the four main pillars through which the IRI exercises coercive power in cyberspace, including the National Information Network (NIN), comprehensive regime of Internet filtering, laws regulating cyber activities, and defensive and offensive capabilities to deter cyber threats at the global level. The IRI's deployment of these pillars, generally speaking, are not unique to it and can be viewed as serving a necessary function. Most countries, in one form or another, utilize intranets for government networks, universities and research centers, and private corporations, though very few do so nationally and as a substitute for the global Internet. Likewise, most have filtering regimes and laws regulating cyber activities in order to block access to criminal content and prosecute online illegal activities or offline crimes facilitated by cyberspace, including the production and distribution of child pornography and illicit trafficking of arms, drugs, and humans. Finally, most countries utilize their cyber capabilities to defend and deter against cyber attacks at the global level.

Yet the way in which the IRI has established and used these pillars of coercive power are problematic in a number of ways. The NIN, for example, can confer a number of benefits to Iranians and the IRI, including higher speeds and greater security from external attack. However, if the NIN is a substitute for the global Internet, rather than a complement, and is therefore used to isolate Iranians, it could limit their ability to flourish through the multitude of uses of the Internet. There are signs that under the Hassan Rouhani administration the NIN is moving toward serving as more of a complement rather than substitute of the global Internet. The filtering regime and laws regulating cyber activities are typically deployed in the IRI as blunt instruments to repress a wide range of online activity and content deemed to be against its religious and

socio-cultural values and political ideals, rather than as scalpels to target undeniably criminal activity, as is the case in many other countries. This not only limits the ability of Iranians to engage in online activities that their peers around the world do as a matter of course, but actually criminalizes a broad spectrum of activities and even ideas that constitute a normal part of life today. Innocuous daily activities like critiquing a particular interpretation of religious values on messaging app, expressing non-violent political ideas in a blog post, or advertising fashion goods and services on a website, may get an Iranian punished under the law. Finally, while many countries exercise coercive cyber power to defend and deter against cyber attacks at the global level, the IRI has the record of using these capabilities against the online platforms of Iranian civil society, as demonstrated during the 2009 Green Movement.

The IRI's use of the four pillars of coercive power is not only problematic, but in the long-term has proven to be of limited effectiveness. Despite the IRI's attempts to restrict and criminalize online content and activities, ordinary Iranians continue to consume content and engage in activities prohibited by the state on a large scale. Furthermore, this approach is not particularly effective in terms of protecting and reinvigorating the country's socio-cultural values and political ideals against foreign ones. This is because a country's ideals and values are not monopolized by the state, but require the input of civil society, including scholars, intellectuals, artists, and the private sector, among others, to keep values and ideals attractive or generate new ones. Yet the IRI's coercive approach to cyberspace actually inhibits civil society's ability to perform this function. A successful approach to this issue requires allowing civil society to rejuvenate a country's existing values and ideals and create new ones to better combat the attractiveness of foreign values and ideals. This will be discussed in greater details in chapter six.

CHAPTER FOUR: THE DEVELOPMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY AND THE IRANIAN ECONOMY

Introduction

As discussed in detail in the theoretical framework chapter of this dissertation, the economy is one of the main sources of power, and cyberspace can impact state-society and international relations by providing a new domain for economic activities and competition. Economic power constitutes the foundation of coercive power, particularly in the contemporary world where building the instruments of coercive power is significantly expensive. Economic power is also one of the foundations of the power embedded in international institutions, which allow a state to exercise power over actors by framing the agendas of these institutions. Moreover, economic power can be generated as part of the interdependence inherent to the global economy, where states with greater economic resources can utilize asymmetries in interdependent economic relationships to achieve their political objectives. Finally, prosperous economy is crucial for providing the commodities and services necessary for the basic functioning and well being of a society, thereby decreasing social tensions arising from economic malaise that can be exploited by foreign adversaries to erode the internal cohesion of a state. Cyberspace is an emerging domain for economic activity, competition, and wealth generation, and thus can significantly contribute to the economic power of a nation.

The Internet economy is estimated to be $4.2 trillion, the equivalent of 5.3 percent of GDP in G-20 economies, while in some of these countries the contribution of the Internet economy is as high as 8 percent of GDP. It is estimated that the Internet economy has grown at an annual rate of

8 percent in the G-20 countries, outpacing all other economic sectors, between 2011 and 2016.[353] Besides the job and wealth creation directly related to Internet infrastructure and services, the Internet economy has enhanced other economic sectors through online retail, online advertising, and research online and purchase offline (ROPO) sales. These have specially helped the small and medium-sized enterprises (SMEs). In the 11 countries of the G-20, SMEs with high level of Internet use have experienced revenue growth 22 percent higher than those with little or no Internet use.[354] Studies show that the Internet has enabled SMEs to access borderless markets, recruit talented staff, and gather data about consumers beyond national borders to create and refine their products and services based on the demands and preferences of consumers abroad. The significant impact of cyberspace on the economy, however, has not evenly materialized across the globe. In fact, we are witnessing a widening digital divide between Global North and Global South countries. Among the major barriers preventing Global South countries from exploiting the economic potential of cyberspace are the under-developed state of Information and Communication Technologies (ICTs) infrastructure, low level of cyber literacy and skills to make effective use of ICTs, and lack of government policies and regulations on economic activities in cyberspace.

According to the 2015 report by Iran's Ministry of Information and Communications Technology, among the 15 major sectors in the Iranian economy, the ICT sector is in the 13th place with a share of 2.12 percent of GDP.[355] This figure suggests that the ICT sector in Iran has risen to

---

[353] Dean, David, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'day, John Pineda, and Paul Zwillenberg. "The Internet Economy in the G-20." *The Boston Consulting Group (BCG)*. Mar. 2012. Web. 01 Mar. 2017. <https://www.bcg.com/documents/file100409.pdf>.

[354] Ibid.

[355] MISI. "Measuring the Information Society of Iran (Islamic Rep.) 2015: ICT and Sustainable Development." *The Official Portal of Measuring Information Society of Iran*. Ministry of Information and Communications Technology of Iran, May 2015. Web. 01 Mar. 2017. <http://mis.ito.gov.ir/documents/20182/34805/MIS_IRAN_2015_EN__940320_pub1-edited940323-1.pdf/6e2d53aa-ca0b-4d2d-91fd-d88340663786>.

become a major sector in the economy during the last decade with a modest contribution to the Iranian GDP. However, considering that this figure does not exclusively represent the size of the Internet economy, but the whole ICT sector, comparing it with the share of the Internet economy in other countries suggests that Iran is lagging behind the developed and even many Global South countries in terms of exploiting the economic potential of cyberspace.

Analyzing four main indexes of ICT development, this chapter conducts a comparative case study between the IRI and countries listed in Iran's 2025 Vision Document. The latter, also called the 2025 Horizon Vision Document of the Islamic Republic of Iran, is a corner-stone development document articulated in the early 2000s by the Expediency Council of the Regime, a high ranking body which, among other things, is tasked to design the IRI's development policies. The 2025 Vision Document was completed by the council and ratified by the supreme leader Ayatollah Ali Khamenei on 4 November 2003.[356] The document emphasizes that the IRI must become ranked first in terms of economy, science, and technology among the countries of the Caucasus, Central Asia, and Middle East regions by the year 2025. The countries targeted in the 2025 Vision Document are: Afghanistan, Armenia, Azerbaijan, Bahrain, Egypt, Georgia, Iraq, Israel, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Lebanon, Oman, Pakistan, Palestine, Qatar, Saudi Arabia, Syria, Tajikistan, Turkey, Turkmenistan, United Arab Emirates, Uzbekistan, and Yemen.

The four indexes studied in this chapter shed light on different aspects of ICT development, highlighting the strengths and weaknesses of the IRI in exploiting the economic potential of cyberspace. These indexes include: 1) The Economist Intelligence Unit and IBM Institute for

[356] CPK. "Sanad-e Cheshm Andaz-e Jomhuri-ye Eslami-ye Iran Dar Ofogh-e 1404 (2025 Horizon Vision Document of the Islamic Republic of Iran)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei*. 04 Nov. 2003. Web. 01 Mar. 2017. <http://farsi.khamenei.ir/message-content?id=9034>.

Business Value's E-readiness Index (ERI); 2) The United Nations' E-government Development Index (EGDI); 3) The World Economic Forum's Networked Readiness Index (NRI); and 4) The International Telecommunication Union's ICT Development Index (IDI). In order to conduct this comparative study, the existing data for all indexes and their respective sub-indexes for the IRI, and all the 2025 Vision targeted countries, have been extracted (Appendix 2-5). These data have been analyzed and featured in the chapter's graphs, which include index values for Iran alongside average index values for the world and 2025 Vision targeted countries. These graphs also illustrate index values of five sample countries from the 2025 Vision list, including Egypt, Israel, Pakistan, Saudi Arabia and Turkey. These countries have been selected because they are the leading powers of the 2025 Vision targeted countries and those with consistently available data across all of the indexes and their respective sub-indexes.

4.1. E-readiness Index (ERI)

Between 2000 and 2010, the Economist Intelligence Unit, in co-operation with IBM Institute for Business Value, assessed the world's 60 to 70 largest economies on their ability to use ICTs for economic and social development. Utilizing major data sources from the Economist Intelligence Unit, Pyramid Research, World Bank, United Nations and World Intellectual Property Organization, among others, more than one hundred qualitative and quantitative criteria of the relationship between the ICT development and economic, political or social development were evaluated in the reports, and an e-readiness index was scored for each country. The index is representative of the country's quality of ICT infrastructure and the ability of consumers, businesses, and governments to use ICT to their benefit by making their economic activities

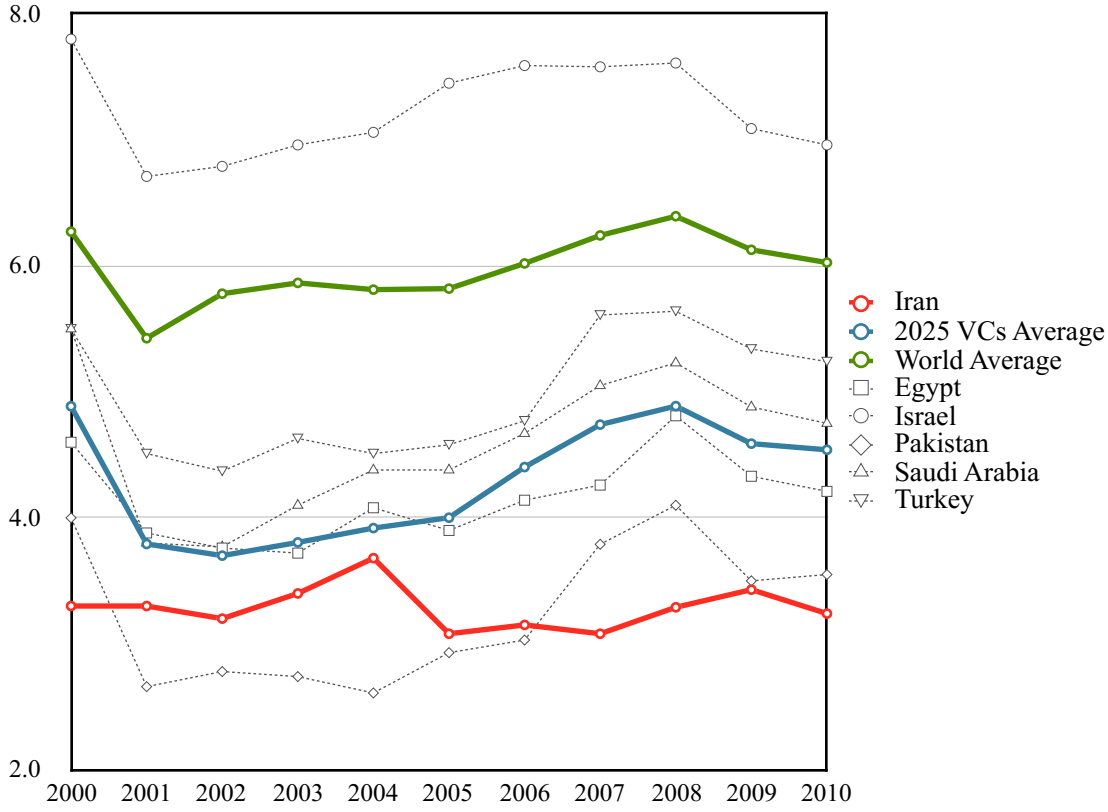
more efficient. Reviewing the e-readiness index shows that Iran was consistently placed among the bottom ten countries, and that in 2007 and 2008 it was the lowest-ranked country among the world's largest economies assessed in the reports (Table 4.1).

Table 4.1: The E-readiness Rankings of the IRI (2000-2010)

Year	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Rank	58	50	53	52	57	59	65	69	70	68	69
Total Countries Ranked	60	60	60	60	64	65	68	69	70	70	70

The e-readiness index of the five sample countries shows that, except for Israel, all are below the average value of the countries covered in the reports. Iran's index value has consistently been lower than the average of the 2025 Vision targeted countries and well below the average of major economies analyzed in the reports (Figure 4.1). Among the five sample countries, Turkey has the highest growth rate, while Iran is the only country to have experienced a declining trend in the e-readiness index. During the Khatami presidency, Iran experienced continuous growth except for the last year, when the index saw a sharp decline. During the Ahmadinejad administration, the IRI had a slower rate of growth, and the country never regained the highest score it had achieved in 2004. Among the sample countries, Iran is ranked second-lowest, only beating out Pakistan before 2006, and fell to the lowest place afterwards. In order to better understand the e-readiness trend in Iran, we must analyze the six primary sub-indexes that constitute the larger e-readiness index. These sub-indexes include: 1) Connectivity and technology infrastructure; 2) Business environment; 3) Social and cultural environment; 4) Legal environment; 5) Government policy and vision; and 6) Consumer and business adoption. The following six subsections introduce each of these sub-indexes and analyze the related data for Iran and all of the 2025 Vision targeted countries.

Figure 4.1: E-readiness Index

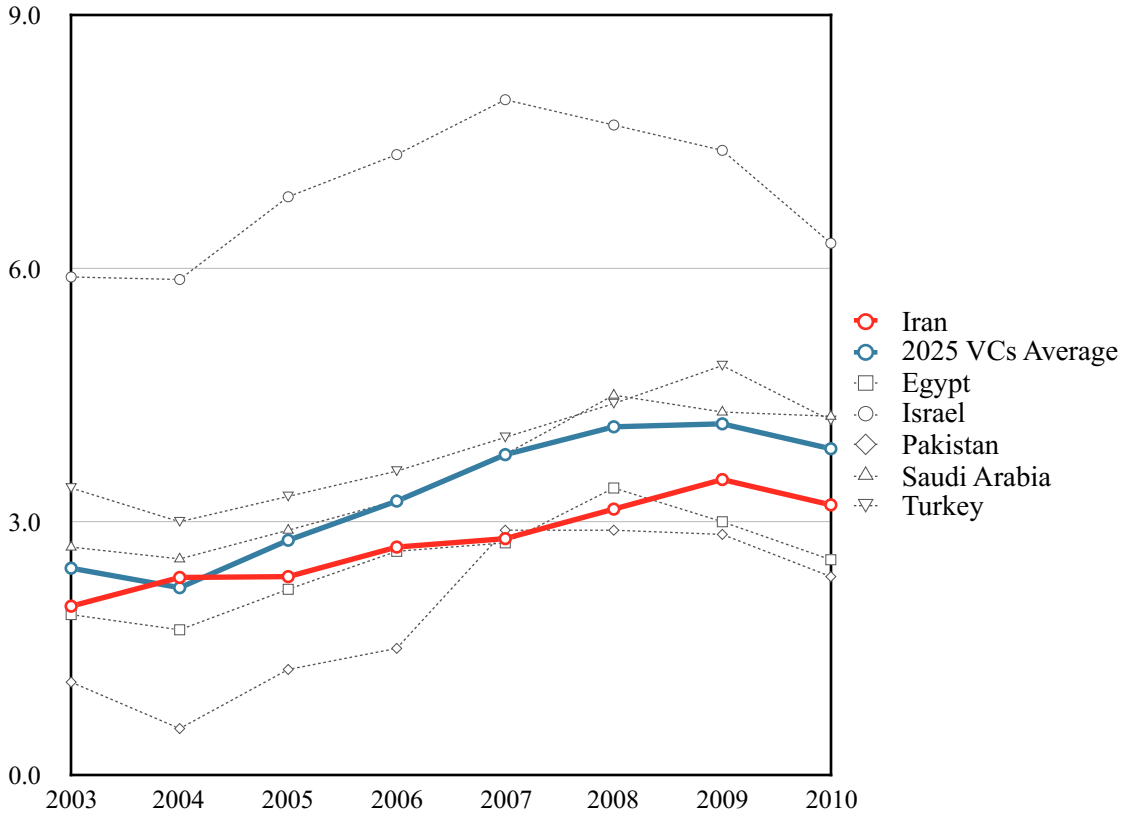


4.1.1 Connectivity and Technology Infrastructure

This sub-index measures the extent and affordability of reliable and secure access to the Internet and mobile networks as a main condition for the development of the Internet economy. The extent of the ICT infrastructure is measured by the percentage of the population using the mobile phones, overall Internet, and broadband Internet with a minimum data stream speed of 256 kb per second. Another factor in measuring the extent of the ICT infrastructure is the international Internet bandwidth, or the capacity of the ICT networks to transmit Internet traffic toward and from other countries. The affordability of ICTs is scored using the cost of broadband Internet per month as a percentage of the average household's median income in each country. The quality of ICTs is measured in terms of the extent to which a country's Internet network uses fiber-optic cables, and

mobile subscribers have access to 3G and 4G services. The security and reliability of the ICTS are measured by the number of secure Internet servers in the country. An analysis of the connectivity and technology infrastructure sub-index data shows that Iran, along with all the five sample countries and the average of the 2025 Vision targeted countries, has experienced a consistent trend of growth between 2003 and 2010 (Figure 4.1.1).

Figure 4.1.1: Connectivity & Technology Infrastructure



Among the five sample countries, Israel has the highest sub-index value with a significant margin over the other sample countries. Although still below the average of the 2025 Vision targeted countries, Iran's connectivity and technology infrastructure sub-index has almost consistently been higher than that of Egypt and Pakistan, while the latter had the highest average growth rate. The

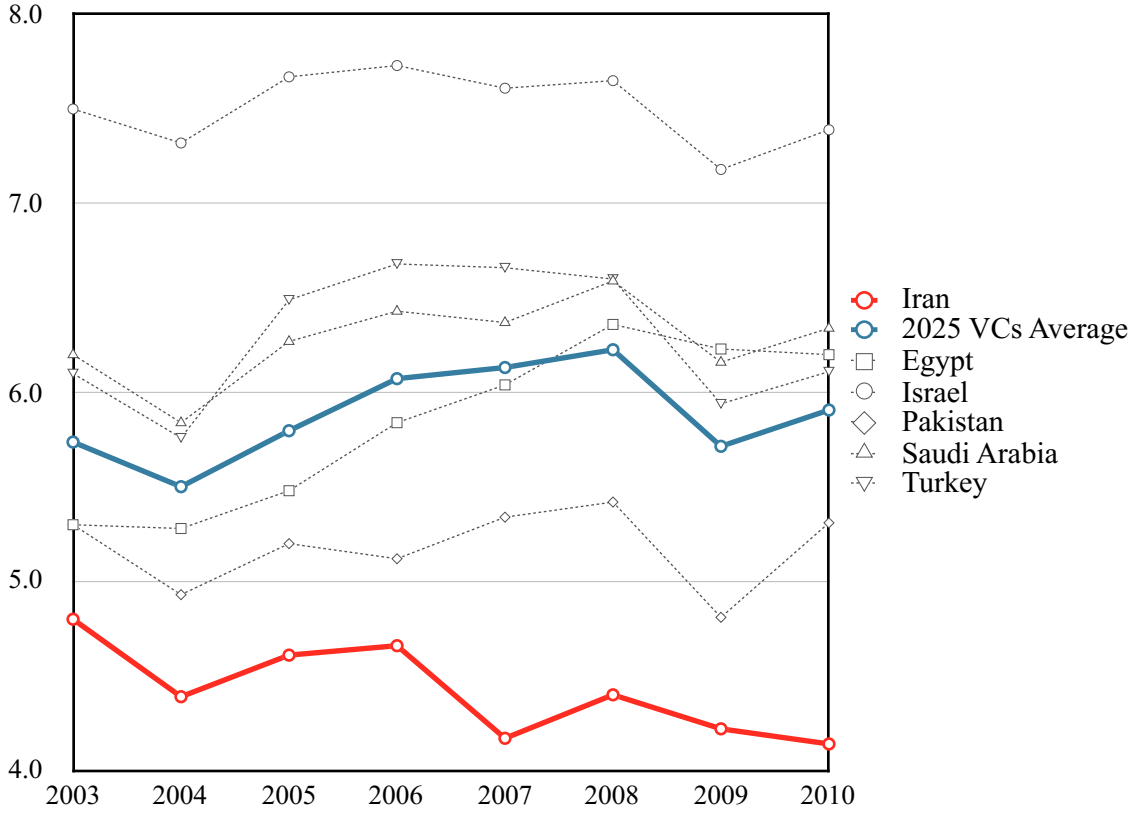
continuous trend of growth in the connectivity and technology infrastructure sub-index indicates that both the Khatami and Ahmadinejad administrations have supported the development of ICT infrastructure in the country, although the extent of this development still lags behind countries such as Israel and Turkey.

4.1.2. Business Environment

This sub-index measures the capacity of a country to create a stable environment for trade and business investment. The country's economic and political stability, market opportunities, taxation regime, private enterprise and foreign investment policies, labour market, and openness to trade and investment are the main components of this sub-index. It is worth noting that the indicators used in this sub-index are related to the economy in general and not exclusively the Internet economy sectors. However, as these macroeconomic criteria have direct impact on all sectors of the economy, including the ones related to Internet economy, this sub-index is considered as a crucially important component of the e-readiness index. As Figure 4.1.2 shows, the IRI's Business environment sub-index has consistently been the lowest among the five sample counties and always below the average of the 2025 Vision targeted countries. Among the sample countries, Egypt and Iran's business environment sub-index values saw the highest growth and decline rates, respectively. The results show that in 2003, in the middle of Khatami's second term, Iran experienced the most favorable business environment and in 2006, after Ahmadinejad's second year in office, the country's business favorability began to decline and reached its lowest point in 2007. This trend can be explained by the shift in domestic economic and foreign policies during this period between the two presidencies. Whereas Khatami demonstrated proper domestic economic management and had a moderate foreign policy which

sought closer integration between Iran and the global economy, this was reversed under Ahmadinejad due to his administration's poor domestic economic management and confrontational foreign policy, which had a negative impact on all sectors of the economy.

Figure 4.1.2: Business Environment

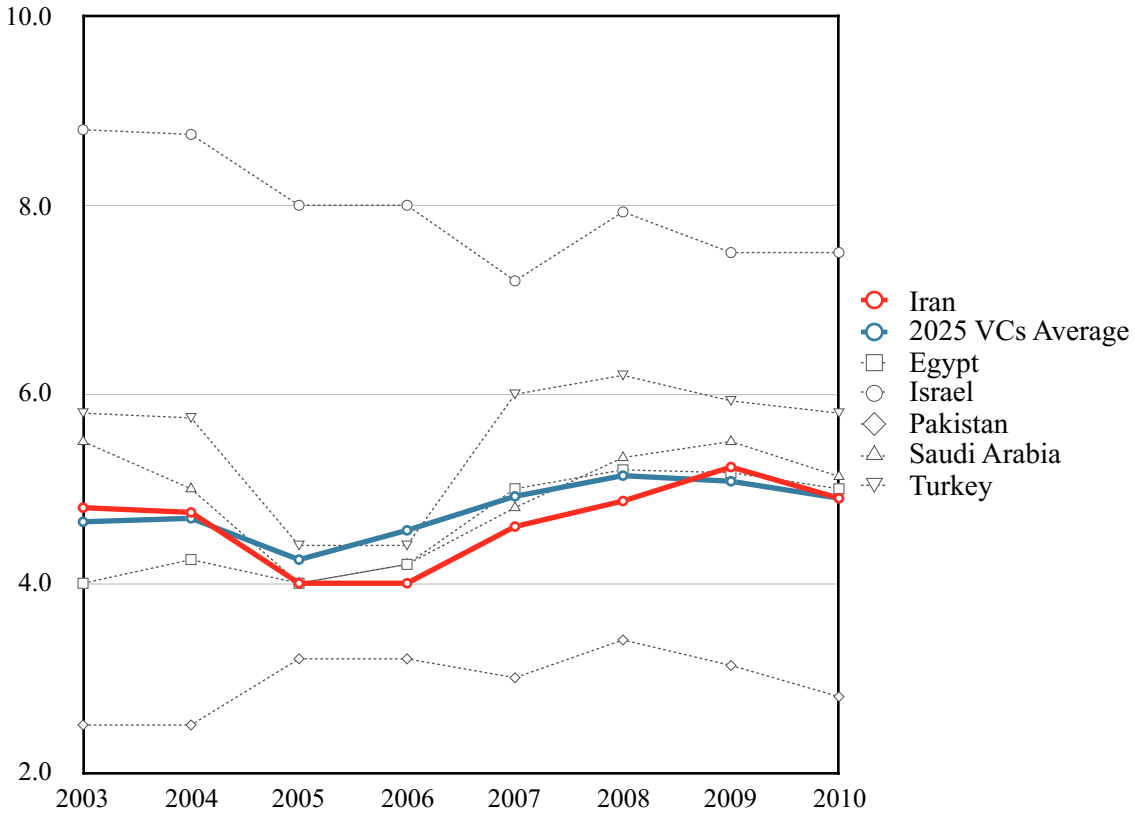


4.1.3. Social and Cultural Environment

This sub-index is indicative of a population's skills and capabilities to make effective use of ICTs. One component of this sub-index is the country's educational level as measured by the gross enrollment in education and school life expectancy, meaning the total number of years of schooling from the primary to tertiary levels. Another component is the population's cyber literacy and work force's technical skills, which are necessary for the effective use of ICTs, and

the extent to which schools and governments support these efforts with educational resources. The degree of entrepreneurship and innovation are the other main components of this sub-index. The former is indicative of the research and development (R&D) expenditure as a percentage of the GDP and number of registered patents and trademarks, while the latter evaluates the extent to which the country fosters creative business activity to create intellectual property and innovative products and industries.

Figure 4.1.3: Social and Cultural Environment



As figure 4.1.3 illustrates, the IRI's social and cultural environment sub-index is quite close to the average of the 2025 Vision targeted countries, but still the second lowest ranked after Pakistan. Among the five sample countries, Egypt has the highest average growth rate while

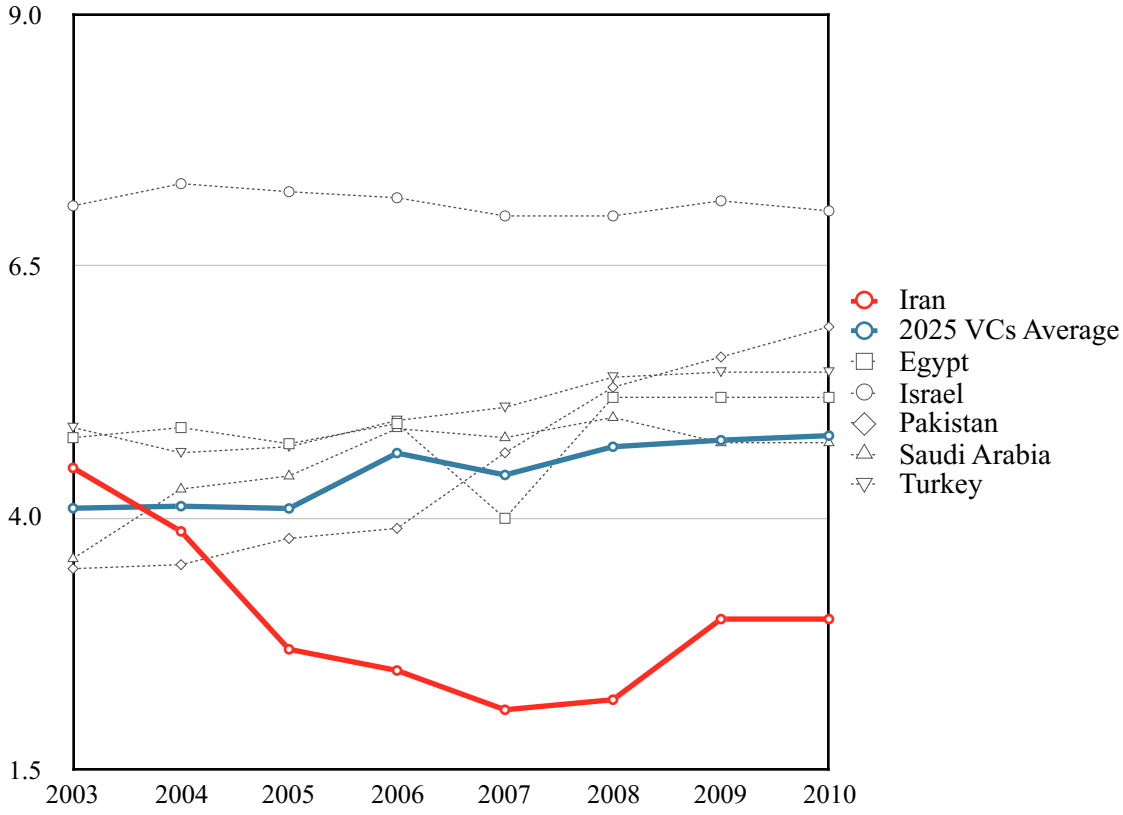
Israel is the only country to have experienced a declining trend in the social and cultural environment sub-index. The figure shows a rising trend in the IRI's sub-index value since 2005, and in the last two recorded years the country was able to close the gap with Egypt and Saudi Arabia. Among the IRI's e-readiness sub-indexes discussed in this subsection, the social and cultural environment sub-index has the lowest gap with the average of the 2025 Vision targeted countries, mainly because of the high rates of both general and cyber literacy in the country. The IRI could have been placed among the top 2025 Vision countries, had other components of the social and cultural environment sub-index, such as the degrees of entrepreneurship and innovation, scored higher.

4.1.4. Legal environment

This sub-index evaluates the effectiveness of a country's legal framework as a key prerequisite for realizing the economic potential of cyberspace. This includes the country's legal framework in general, and the laws governing ICTs in particular, which directly impact how people use ICTs to communicate and transact business online, including laws relating to cybercrime, data privacy, and online consumer protection. The countries with effective legal frameworks that foster the Internet economy have little bureaucracy to interfere with the registration of new businesses and a minimum level of restrictions when it comes to access to information. As figure 4.1.4 demonstrates, the IRI's legal environment sub-index value has consistently declined between 2003 and 2008, with only minor improvement in subsequent years. Except for Israel and Iran, all sample countries have experienced growth, with Pakistan and Iran having the highest growth and decline rates, respectively. Figure 4.1.4 also shows that Iran is the lowest-ranked among the

sample countries after 2004, and the gap with the 2025 Vision targeted countries' average has since widened. The main reasons behind this decline are the state bureaucratic structures that impede business registration, lack of effective laws for the conduct of business online, restrictiveness of laws regulating content generation and communication in cyberspace, and extensive regime of Internet censorship which intensified during the Ahmadinejad presidency.

Figure 4.1.4: Legal environment



4.1.5. Government Policy and Vision

One indicator of ICT development is the degree to which a government supplies its citizens with a clear roadmap for ICT development and leads by example in adopting ICTs into bureaucratic machinery to optimize its operations and deliver services to citizens. The government policy and

vision sub-index assesses government policies and strategies for ICT development, the government's capacity to use technologies to provide public services and information about government agencies to the public, and the extent to which governments utilize the ICTs to provide the public with the opportunity to engage with the government officials and organizations in the policy making processes.

Figure 4.1.5: Government Policy and Vision

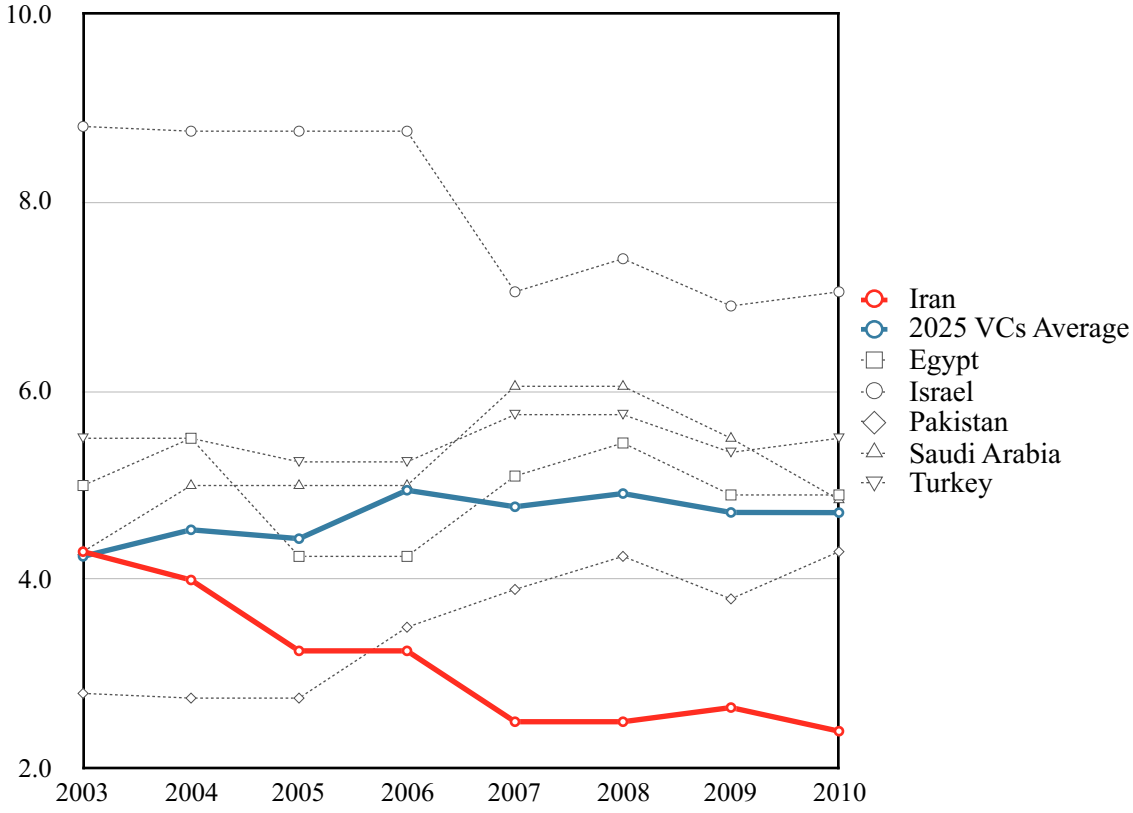


Figure 4.1.5 illustrates that, among the sample countries, Pakistan's government policy and vision sub-index value saw the highest growth rate, while Israel had the highest rate of decline. The IRI's government policy and vision sub-index value has consistently declined since 2003, and after 2006 Iran was the lowest-ranked among the sample countries. In fact, among the IRI's

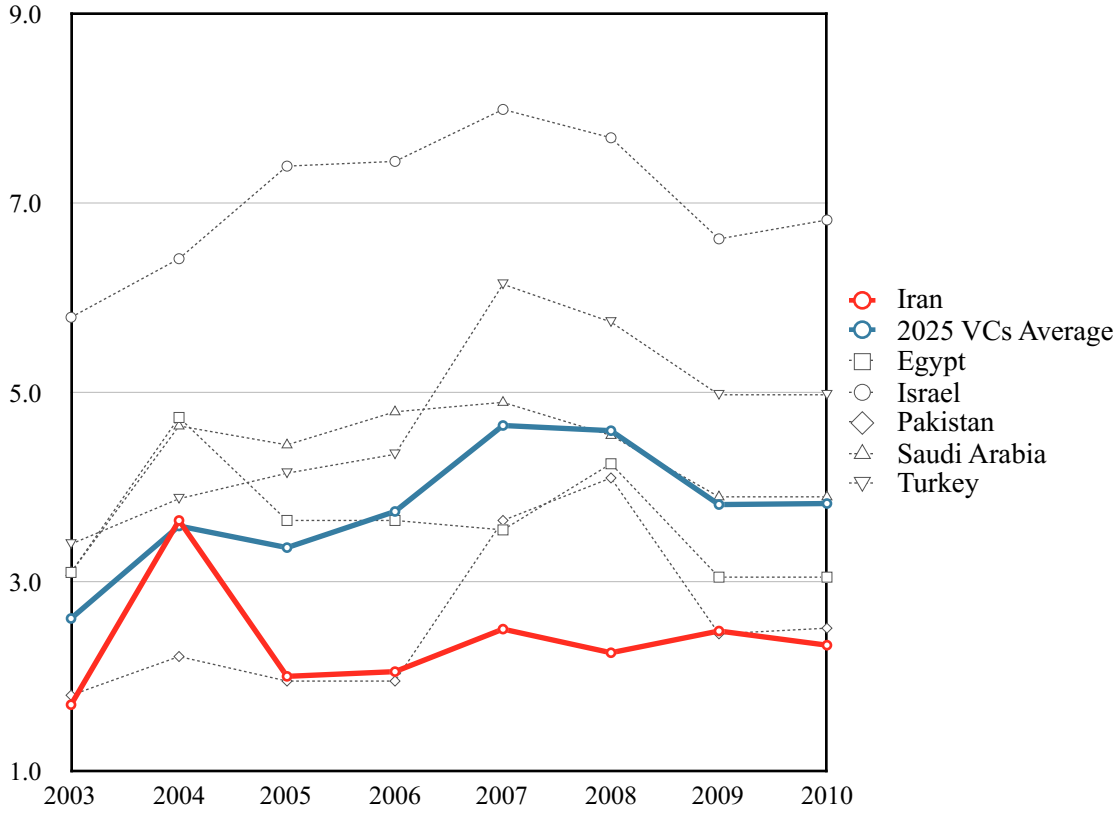
e-readiness sub-indexes discussed in this subsection, the government policy and vision value saw the highest rate of decline, and the gap between the IRI and the 2025 Vision targeted countries' average has steadily widened. Although both the Khatami and Ahmadinejad administrations emphasized the merits of e-government for optimization of the state bureaucratic machinery and fostering governmental services for the public, the sub-index value suggests that they were quite unsuccessful in the actual development of e-government. Although Iran experienced modest progress in utilizing ICTs to provide services and information about government agencies to the public, the government's dearth of ICT use to provide the public with opportunities to engage in the policy making processes lead to a steady decline of the government policy and vision sub-index value.

4.1.6. Consumer and Business Adoption

All the sub-indexes discussed so far have evaluated various necessary conditions for the development of the Internet economy in a country. The consumer and business adoption sub-index measures the extent to which these conditions translate into actual utilization of ICTs by individuals and companies to transact business online. To assess the extent of ICT utilization, this sub-index measures business and consumer spending on ICT services, the degree and range of individual use of internet features and online purchasing activities, and the scope of individual and business use of public services made available online by the government. Figure 4.1.6 shows that, except for Egypt, all sample countries along with the 2025 Vision targeted countries's average have experienced growth, with Turkey having the highest rate of growth. Iran's consumer and business adoption sub-index value has almost consistently been below the 2025 Vision targeted countries' average, and after 2006 Iran was ranked as the lowest country among

the sample countries. As noted above, this sub-index is indicative of the actual utilization of ICTs, conditioned by the e-readiness criteria discussed in previous sub-indexes. As a result, the unsatisfactory performance of the IRI in previous sub-indexes, specifically the business environment, legal framework, and government policy and vision sub-indexes, is ultimately reflected in the country's poor performance in terms of the actual use of ICTs by individuals and companies to transact business online.

Figure 4.1.6: Consumer and Business Adoption



4.2. E-Government Development Index (EGDI)

Since 2003, the United Nations Department of Economic and Social Affairs (UNDESA) has published the E-Government survey to analyze the progress of e-government development and

its contribution to the realization of the Millennium Development Goals (MDGs), and more recently Sustainable Development Goals (SDGs). The survey assesses data from all United Nations Member States to track the progress of e-government via the E-Government Development Index (EGDI), which is indicative of the capacity of governments to utilize ICTs to deliver public services in the following five sectors: education, health, labour and employment, finance, and social welfare. The EGDI between 2001 and 2016 shows a rapid growth in the implementation of e-government across the globe. In the 2016 survey, 29 countries scored "very-high", with EGDI values 0.75 to 1, compared to only 10 countries in 2003. Whereas in 2003 over 73 percent of countries scored "medium EGDI" or "low- EGDI", with EGDI values between 0.25 to 0.5 and less than 0.25, respectively, this figure has been reduced to 51 per cent in 2016. Despite overall growth, the wide gap between different regions of the world has remained unchanged since 2001. The 2016 survey results show the largest gap to be between African countries, with a low EGDI average of 0.2882, and European countries, with a high EGDI average of 0.7241. With an average EGDI of 0.4154, the Oceania region is below the global average of 0.4623, while Asia and the Americas with average EGDI values of 0.5132 and 0.5245, respectively, are narrowly above the global average.[357]

As compared to the E-readiness Index discussed in the previous subsection, EGDI is more focused on the utilization of ICT for economic and social development by governments rather than the business sector or citizens. Additionally, this index covers all of the 2025 Vision targeted countries over a longer period of time, helping to capture a better idea about the IRI's standing

[357] UN. "UN E-Government Survey 2016." *The United Nations*. 2016. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>.

both in the world and among the targeted countries in terms of ICT development. It should be noted, however, that the EGDI has experienced a number of changes in its core methodology over the years. This has created discontinuities in our ability to track data over time, specifically in the Online Service and E-Participation sub-indexes discussed later on. Nonetheless, the EGDI is still useful for demonstrating overall historical trends and the relative standing of each country year to year in terms of e-government development.

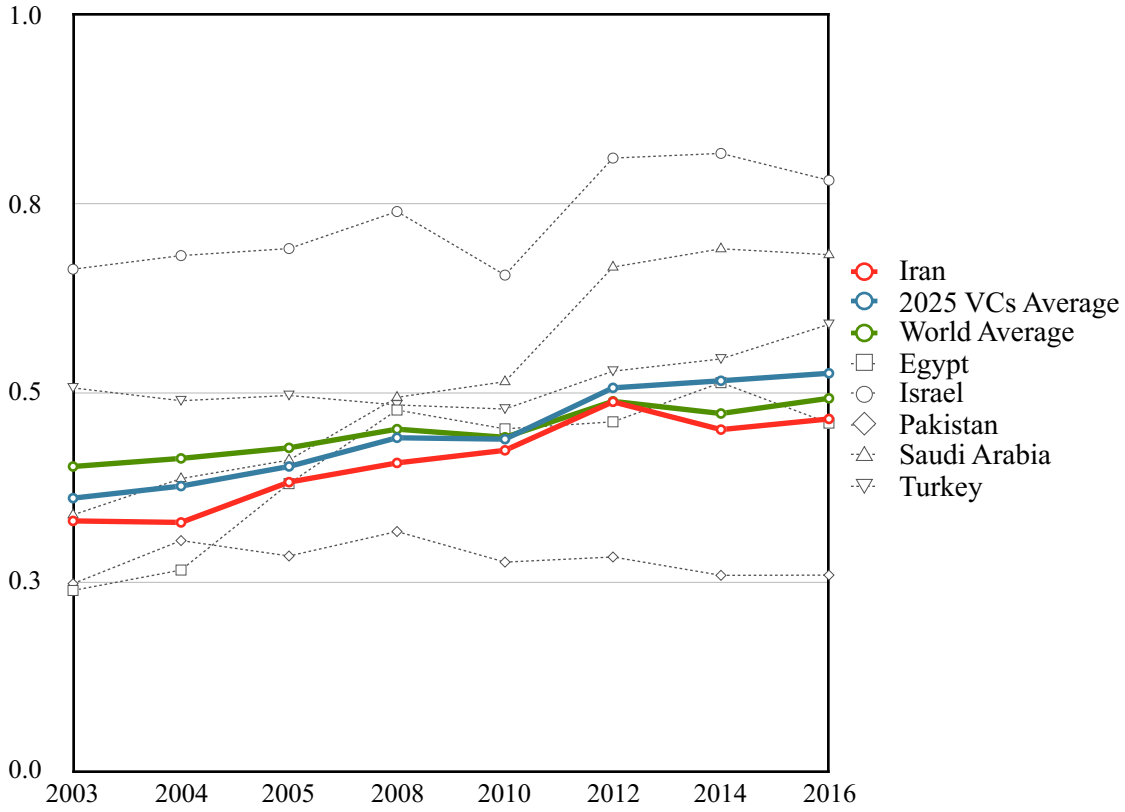
Table 4.2: The E-Government Development Rankings of the IRI (2003-2016)

Year	2003	2004	2005	2008	2010	2012	2014	2016
Rank	107	115	98	108	102	100	105	106
Total Countries Ranked	173	178	179	182	184	190	193	193

The EGDI rankings between 2003 and 2016 shows that the IRI's best and worst rank is 98 in 2005 and 115 in 2004, respectively, and except for 2005 and 2012 the IRI has never been ranked among the top 100 countries worldwide (Table 4.2). As figure 4.2 shows, Iran, Egypt and Turkey's index values saw modest growth close to the average of the 2025 Vision targeted countries. Iran has been constantly below the world average while Israel and Turkey are the only two sample countries that have consistently been above the world average. Among the sample countries, Saudi Arabia has the highest average growth rate, while Pakistan at the bottom is the only country that experienced a declining trend in the e-government development index. The next subsection will introduce and analyze the three primary sub-indexes of EGDI to better understand e-government development trends in the IRI and compare it with the 2025 Vision targeted countries. These sub-indexes include: Telecommunications Infrastructure Index (TII);

Human Capital Index (HCI); and the Online Service Index (OSI). The last subsection will introduce and analyze the supplementary index of E-participation.

Figure 4.2: E-Government Development Index

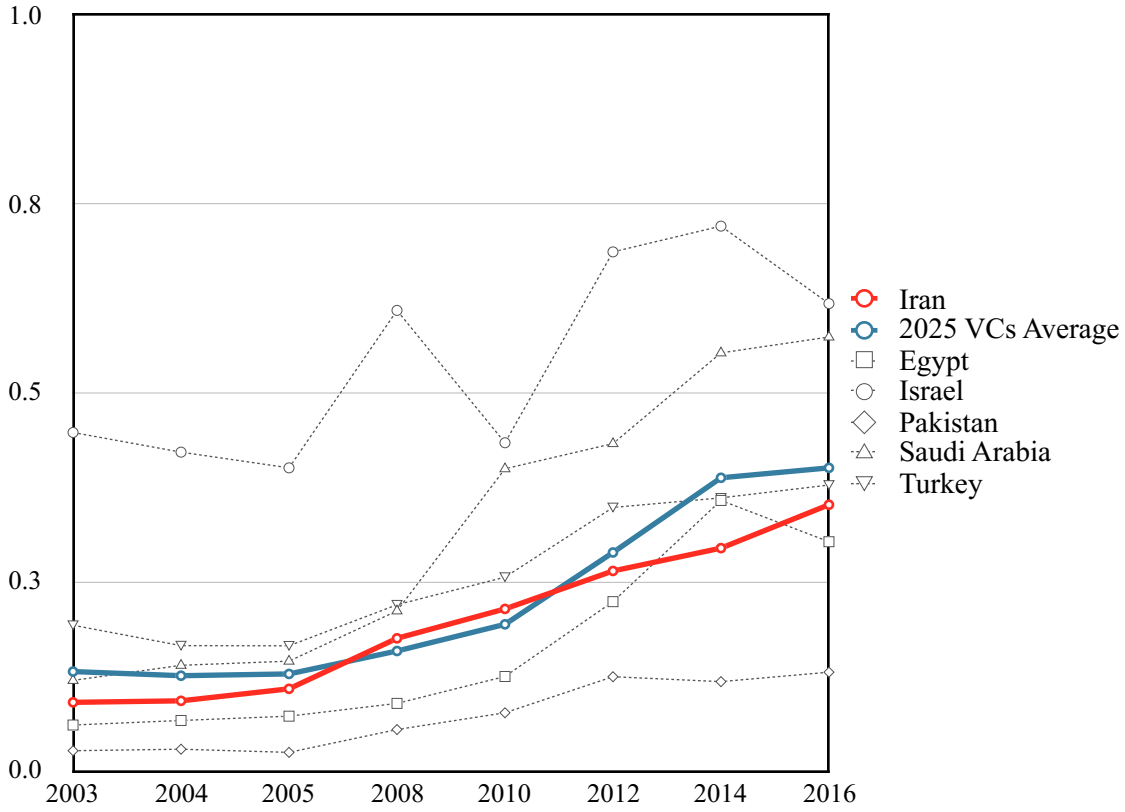


4.2.1. Telecommunications Infrastructure Index (TII)

This sub-index evaluates the development status and capacity of a country's ICT infrastructure based on five indicators: estimated internet users per 100 inhabitants; number of main fixed telephone lines per 100 inhabitants; number of mobile subscribers per 100 inhabitants; number of wireless broadband subscriptions per 100 inhabitants; and number of fixed broadband subscriptions per 100 inhabitants. Similar to the ERI's connectivity and technology infrastructure sub-index discussed above, the TII sub-index is indicative of the level of development of ICT

infrastructure. The main difference between the two sub-indexes is that the former also evaluates the affordability, reliability, and security of ICT infrastructure, while the latter does not.

Figure 4.2.1: Telecommunications Infrastructure Index



Reviewing TII between 2003 and 2016 shows that all of the sample countries, along with the average of the 2025 Vision targeted countries, witnessed growth, with Saudi Arabia and Pakistan experiencing the highest and lowest rates of growth, respectively (Figure 4.2.1). The IRI's sub-index value has been almost consistently close to the 2025 Vision targeted countries' average and above those of Pakistan and Egypt. The sub-index also shows consistent growth during the last three consecutive presidential administrations in Iran. Comparing the main factors contributing to growth in the TII sub-index value, the data indicates that progress in the number of fixed and

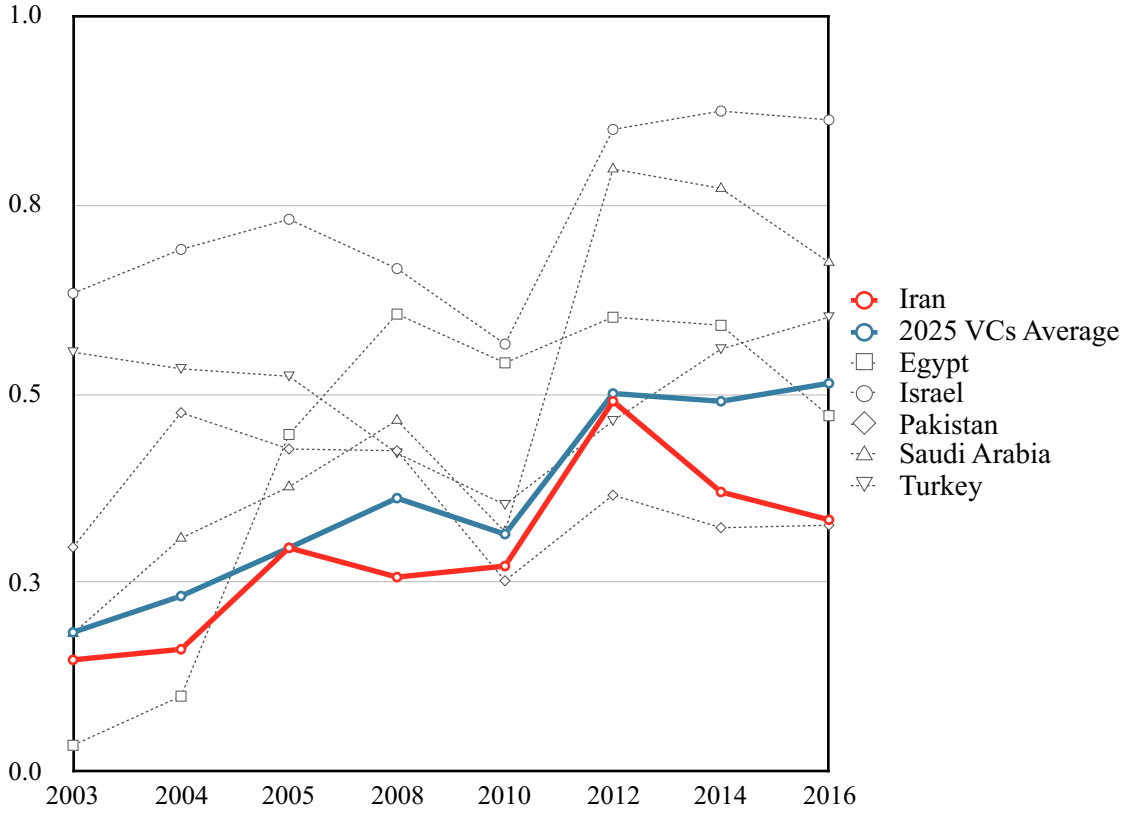
wireless broadband subscribers has been the main factor behind the growth under Rouhani, while the increase in the number of internet users, fixed telephone, and mobile subscribers was the main contributor to the growth under the Ahmadinejad and Khatami administrations.

4.2.2 Online Service Index (OSI)

This sub-index evaluates the scope and quality of online services provided by the government. To measure this sub-index for 2016, dozens of UN experts and volunteers assess each country's national websites in the native language, including the national and e-services portals and the websites of the ministries of education, labour, social services, health, finance, and environment. The UN experts and volunteers assess whether the features and information related to public services could be easily found and accessed, and how the intended beneficiaries could effectively benefit from online services available on government websites. The OSI sub-index between 2003 and 2016 shows that Iran experienced the highest growth rates in the 2004-2005 period under Khatami and in the 2010-2012 period under Ahmadinejad (Figure 4.2.2). The sub-index also shows that Iran has been consistently below the average of the 2025 Vision targeted countries, and that it was the lowest ranked among the sample countries during the first term of the Ahmadinejad administration. Despite Rouhani's emphasis on ICT development in the country, the country has experienced a declining trend in the sub-index value under his administration to such an extent that in 2016 Iran is the second lowest country among the sample countries, with only Pakistan behind it by a very thin margin. It's worth mentioning that part of the sharp decline in the sub-index in 2010 is due to changes in methodology by the United Nations Department of Economic and Social Affairs. Due to these changes, the sub-index name changed from the "web

measure index" to the "online service index" in 2010. Despite the change in methodology, however, since both versions of sub-index share the main components, the sub-index is still illustrative of the overall trend between 2003 and 2016.

Figure 4.2.2: Online Service Index

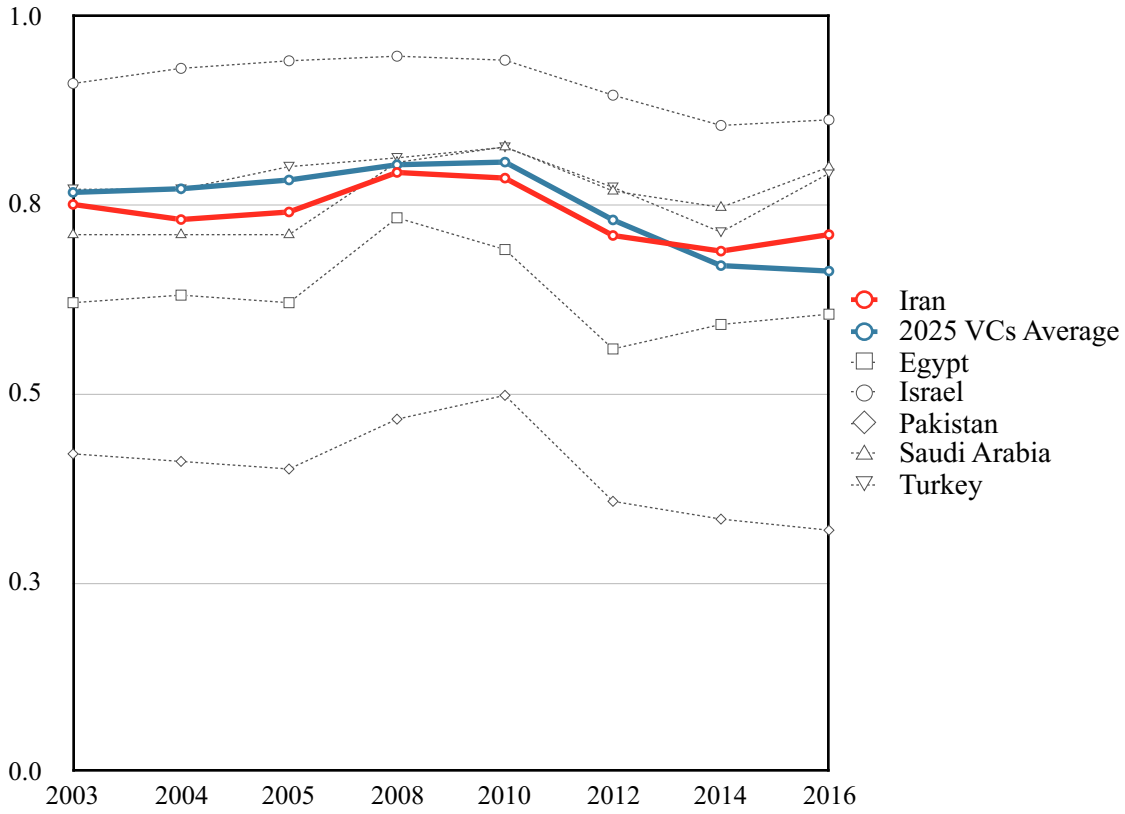


4.2.3 Human Capital Index (HCI)

This index is indicative of the population's ability to access and utilize ICTs in order to benefit from the government public services available online. The HCI consists of four components: adult literacy rate; the combined primary, secondary and tertiary gross enrollment ratio; expected years of schooling; and average years of schooling. The first two components have been used in EGDI surveys between 2002 and 2014. In order to strengthen the HCI, the 2014 EGDI survey

introduced two new components to the index, namely expected years of schooling (i.e. the total number of years of schooling that a child of a certain age can expect to receive in the future), and average years of schooling (i.e. the average number of years of education completed by a country's population aged 25 years and older).

Figure 4.2.3: Human Capital Index



Human Capital Index values between 2003 and 2016 shows that, except for Saudi Arabia, all sample countries along with the 2025 Vision targeted countries' average have experienced a declining trend, with Pakistan experiencing the highest rate of decline (Figure 4.2.3). Iran's HCI value has consistently been above Pakistan and Egypt, and close to the average of the 2025 Vision targeted countries. The figure shows a major decline in HCI value during the second term

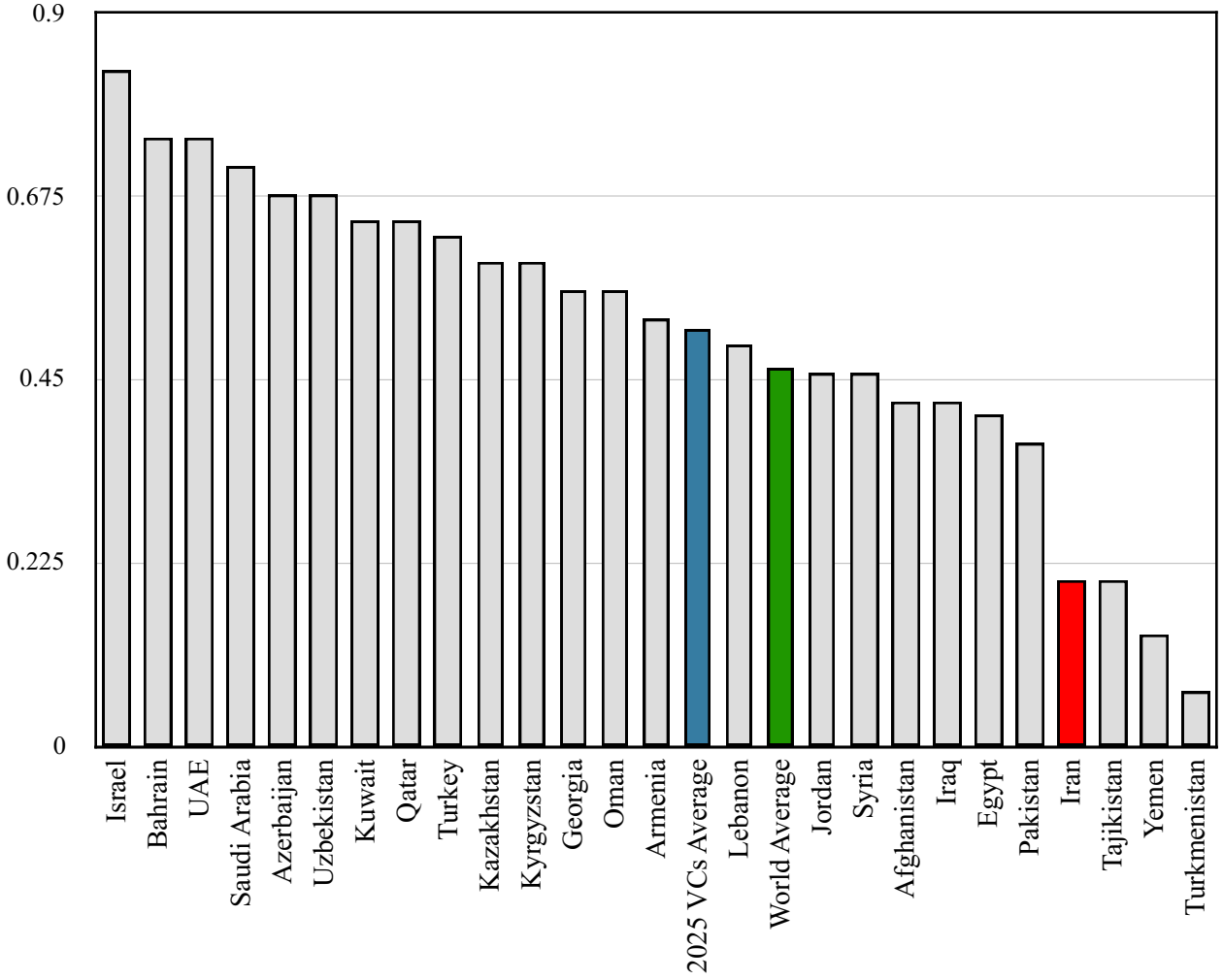
of the Ahmadinejad administration, which is the main reason behind the average decline of the country in the whole period between 2003 and 2016. Under the Rouhani administration the country returned to a growth trend and, for the first time since the start of data collection in 2003, Iran has scored higher than the 2025 Vision targeted countries' average in the 2014-2016 period.

4.2.4 E-Participation Index (EPI)

EPI is a supplementary index to the E-Government survey that focuses on the utilization of ICT by the government for providing citizens with public information (e-information sharing), public consultation on policies and services with citizens (e-consultation), and empowering the public in government decision-making processes (e-decision-making). The main criteria evaluated by this index include: citizens' rights to access the government information, availability of government information online, government use of online tools including social media platforms, online polls and online discussion forums to foster citizens contribution to the policy making processes and designing public services. It is worth noting that the main components and methodologies of the e-participation index have been regularly modified since 2003 and, as a result, tracking the e-participation values presented in all editions of the survey is virtually meaningless. Instead, figure 4.2.4 shows the 2016 rankings of Iran and all countries targeted in the 2025 Vision Document. The figure shows that Iran's e-participation value is below both the world and the 2025 Vision targeted countries' averages. In fact, among all the 2025 Vision targeted countries, Iran and Tajikistan are the third-lowest, following only Yemen and Turkmenistan. The country's poor results in terms of e-participation highlights the lack of vision and will from most governmental organizations in utilizing ICTs to share public information and

deliver services to citizens. Even in cases where governmental organizations have sought to do so, poor website design and low Internet access speeds have impeded the effective utilization of ICTs by the public to access government information and services. Moreover, governmental organizations' websites are rarely equipped with online tools such as social media, online polls, and online discussion forums to consult with the citizenry on public policies and foster public participation in the policy making processes.

Figure 4.2.4: 2016 E-Participation Index Rankings



4.3. Networked Readiness Index (NRI)

Since 2000, the World Economic Forum has published The Global Information Technology Report (GITR) to assess the state of network preparedness of countries by using the Networked Readiness Index (NRI). The conceptual framework behind the NRI demonstrates that a high-quality political and regulatory environment, and innovation and business climate enhance both ICT readiness and the effective usage of ICTs by the government, business sector, and public. Accordingly, a high quality environment for ICT development, readiness and effective use, are the three preliminary factors highlighted in the NRI conceptual framework. However, this framework emphasizes that these three factors are not ends in themselves, and what should ultimately be evaluated is the impact that these factors have on the economy and society. The economic and social impact of ICT is therefore a complementary factor to the NRI conceptual framework. By analyzing these four factors, the NRI provides a clear understanding of the state of ICT in the world and the widening digital divide between Global North and Global South countries. The NRI results between 2001 and 2016 have consistently underlined the strong association between the level of income in a country and its NRI value. In 2015 NRI ranking, for instance, high-income economies took the first 31 places, and among the top 50 countries only 6 were not high-income economies. On the other hand, 26 of the 30 worst-performing countries in the 2015 rankings, were low-income or lower-middle-income countries.[358] Since the Global Information Technology Report did not include Iran before 2011, this section analyzes NRI data between 2011 and 2016. During this period, the IRI's best and worst rank was 92 among 139 countries in 2016 and 104 among 142 countries in 2012, respectively (Table 4.3).

---

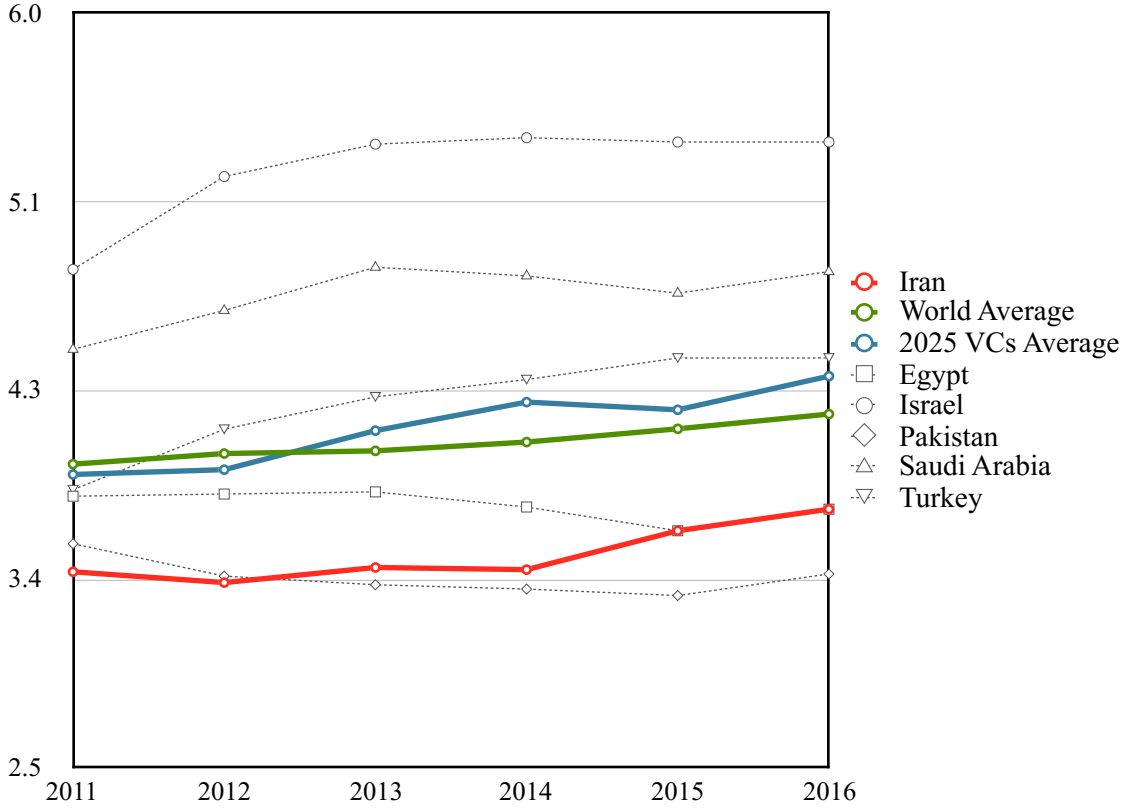
[358] WEF. "The Global Information Technology Report 2015: ICTs for Inclusive Growth." *The World Economic Forum*. 2015. Web. 01 Mar. 2017. <https://reports.weforum.org/global-information-technology-report-2015/>.

Table 4.3: The Networked Readiness Rankings of the IRI (2011-2016)

Year	2011	2012	2013	2014	2015	2016
Rank	101	104	101	104	96	92
Total Countries Ranked	138	142	144	148	143	139

As figure 4.3 shows, among the sample countries, Israel has consistently been at the top, while in 2011 and 2012 Iran, and since 2013 Pakistan, had the lowest NRI scores, respectively. Except for Egypt and Pakistan, all sample countries have experienced growth in the time period between 2011 and 2016, with Turkey having the highest rate of growth. Among the sample countries, Iran, Egypt, and Pakistan have been constantly below both the 2025 Vision targeted countries' and world averages by a considerable margin. Compared to the Ahmadinejad administration's

Figure 4.3: Networked Readiness Index



second term, the country has experienced considerably faster growth rate under the Rouhani administration since 2013. As discussed above, the ICT environment, readiness, usage and impact are the main factors of the NRI framework. Each of these factors in turn corresponds to its own sub-index in the NRI which will be discussed in the following subsections.

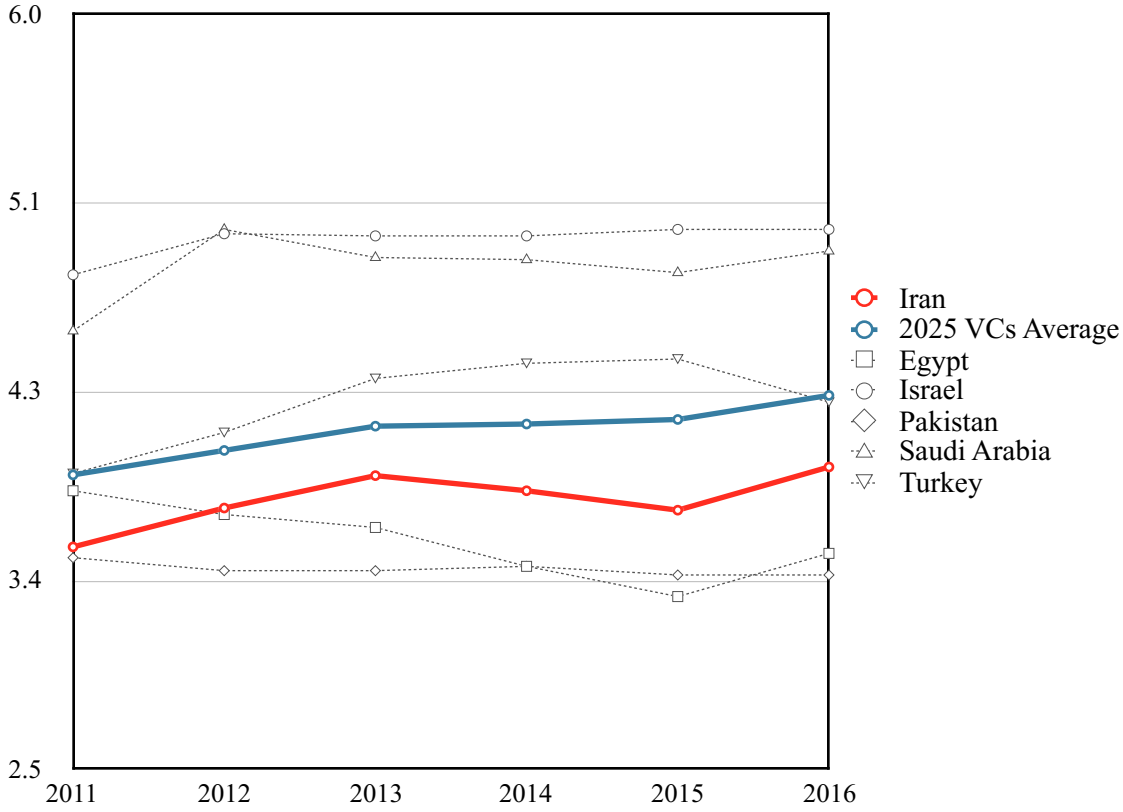
4.3.1 Environment sub-index

This sub-index assesses the extent to which the political and business conditions in a country facilitate ICT entrepreneurship, innovation, and development. The first component of this sub-index, political and regulatory environment, measures the capacity of a country's political and legal systems to promote ICT development based on the "extent of intellectual property rights protection, the prevalence of software piracy, the efficiency and independence of the judiciary, the efficiency of the law-making process, and the overall quality of regulations pertaining to ICTs".[359] The second component is the business and innovation environment, which measures the capacity of the business climate to support entrepreneurship in information and communication technologies. In so doing, this component assesses a country's taxation regime, bureaucratic red tape that impedes the ease of starting and conducting business, the intensity of competition in the business sector, and the demand for innovative products and availability of venture capital to fund their production. A review of the environment sub-index data between 2011 and 2016 shows that Iran and all of the sample countries, except for Pakistan and Egypt, have experienced growth, with Turkey and Pakistan seeing the highest growth and decline rates, respectively (Figure 4.3.1). The IRI's sub-index value has been almost consistently below the

[359] Ibid. p.5.

2025 Vision targeted countries' average and above Pakistan and Egypt. The sub-index also shows a growth trend in the last two years of the Ahmadinejad administration, while during the first two years of the Rouhani administration the sub-index value declined. This trend has been reversed in the 2015-2016 period, with the country gaining its highest score in 2016.

Figure 4.3.1: Environment Sub-index



Comparing the results of the political and regulatory environment with the business and innovation environment shows that the former's low value is the main reason behind the IRI's overall poor performance in the environment sub-index. As Table 4.3.1 shows, the business and innovation environment value has steadily increased since 2012, while the political and regulatory environment value saw a sharp decline between 2013 and 2015. As most of the

criteria assessed in the political and regulatory environment component rely on an effective and independent legal system, shortcomings of other branches of government in the country, namely the legislature and judiciary, have been reflected in the low political and regulatory environment scores. Iran's judiciary is not independent and its parliament has not only passed laws which have yet to prove helpful to ICT development, but have actually encumbered its growth (this is discussed in detail in chapter three). Therefore, even the modest progress made by the executive branch of the IRI in the business and innovation environment to improve the country's overall environment sub-index has been, to some extent, nullified by the actions of other centers of power in the IRI.

Table 4.3.1: The Environment Sub-index Rankings and Values of the IRI (2012-2016)

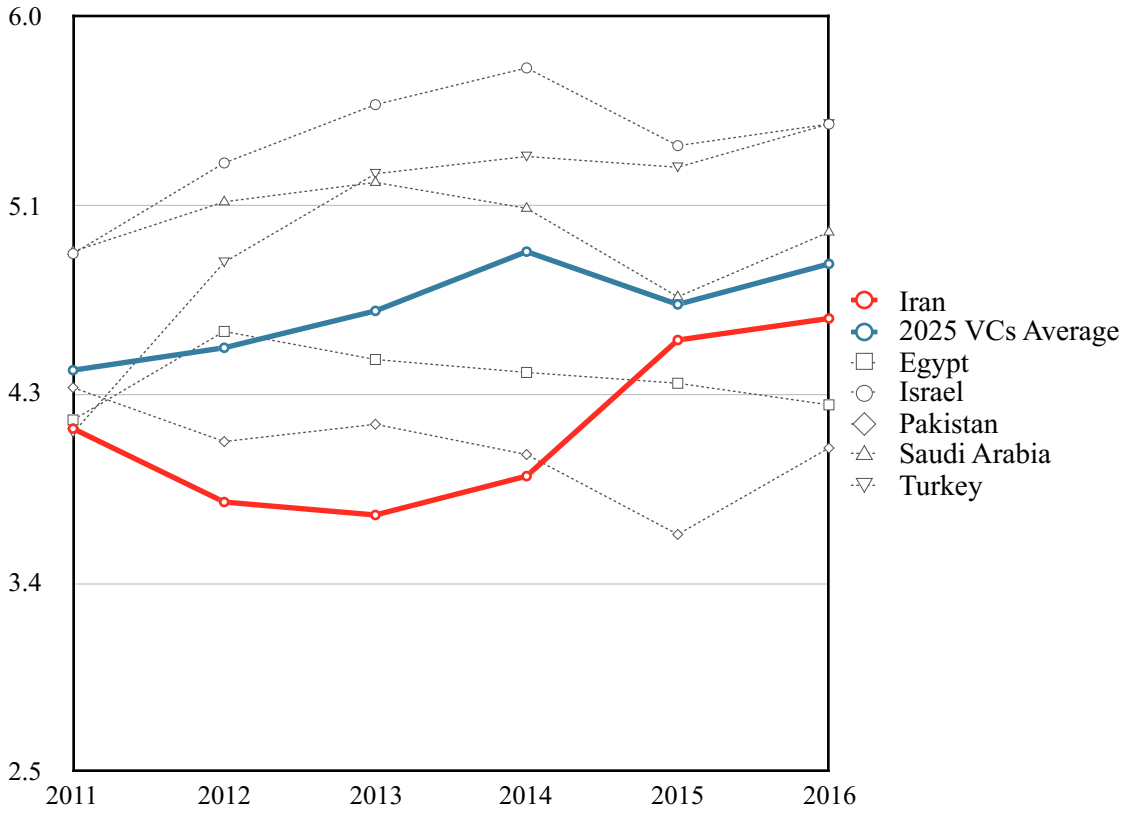
Year	2012	2013	2014	2015	2016
Political and Regulatory Environment Rank	78	67	86	100	91
Political and Regulatory Environment Value	3.57	3.70	3.53	3.4	3.5
Business and Innovation Environment Rank	81	80	86	86	76
Business and Innovation Environment Value	3.85	4.03	4.04	4.1	4.2

4.3.2 Readiness sub-index

The readiness sub-index measures the country's capacity to make effective use of ICTs based on three main factors. The first factor captures the state of a country's ICT infrastructure, including mobile network coverage, international Internet bandwidth, secure Internet servers, and the infrastructure that ICT development is dependent upon, such as electricity production. The second factor assesses the affordability of ICTs in a country by measuring the costs of ICT

services, including mobile and broadband Internet. The third factor measures the skills that the public requires to make effective use of ICTs by taking into account the enrollment rate in secondary education, the overall quality of the education system, and the adult literacy rate. The readiness sub-index values between 2011 and 2016 show that the IRI, Israel, Turkey and Saudi Arabia, along with the 2025 Vision targeted countries average, have experienced growth (Figure 4.3.2). Israel was ranked highest for the longest time in this period, but Turkey, which experienced the highest growth rate among the sample countries during 2011-2016, came to share the top position with Israel in 2016. Iran's readiness sub-index value has been consistently below the 2025 Vision targeted countries's average, and Iran was the lowest ranked country among the sample countries between 2011 and 2014. The figure also shows that the IRI's readiness sub-index declined under Ahmadinejad, but this trend has reversed under Rouhani.

Figure 4.3.2: Readiness Sub-index



As Table 4.3.2 illustrates, among the three main factors of the readiness sub-index, the sharp rise in the affordability value was the main reason behind the increase in Iran's sub-index value since 2013. This is indicative of the successful policies adopted by Rouhani administration to reduce the cost of ICT services in the country. These policies led to an unprecedented improvement in the country's ranking in terms of the affordability of ICT from 114 in 2012 to 37 in 2016. In terms of the state of ICT infrastructure and people's skills to make effective use of ICTs, however, no meaningful differences is observed between the two Iranian administrations.

Table 4.3.2: The Readiness Sub-index Rankings and Values of the IRI (2012-2016)

Year	2012	2013	2014	2015	2016
Infrastructure Rank	99	97	103	97	101
Infrastructure Value	3.16	3.13	3.14	3.0	3.0
Affordability Rank	114	115	118	46	37
Affordability Value	3.27	3.13	3.74	5.8	6.0
Skills Rank	81	69	85	85	80
Skills Value	4.82	4.79	4.73	4.7	4.8

4.3.3 Usage sub-index

This sub-index gauges the level of ICT adoption by individuals, businesses, and government. The individual usage component of the sub-index measures the level of diffusion of ICTs among the population by taking into account the mobile penetration rate, personal computer ownership rate, and number of individuals using the Internet in general, and social networks in particular. The second component captures the extent to which the business sector uses ICTs in their operations, including the business-to-business (B2B) and business-to-consumer (B2C) operations. This component also assesses the capacity of the business sector to develop

innovative technologies by measuring the number of patent applications under the Patent Cooperation Treaty (PCT), among others. The third component, assesses the capacity of the government in "developing and implementing strategies for ICT development, as well as in using ICTs, as measured by the availability and quality of government online services".[360]

Figure 4.3.3: Usage Sub-index

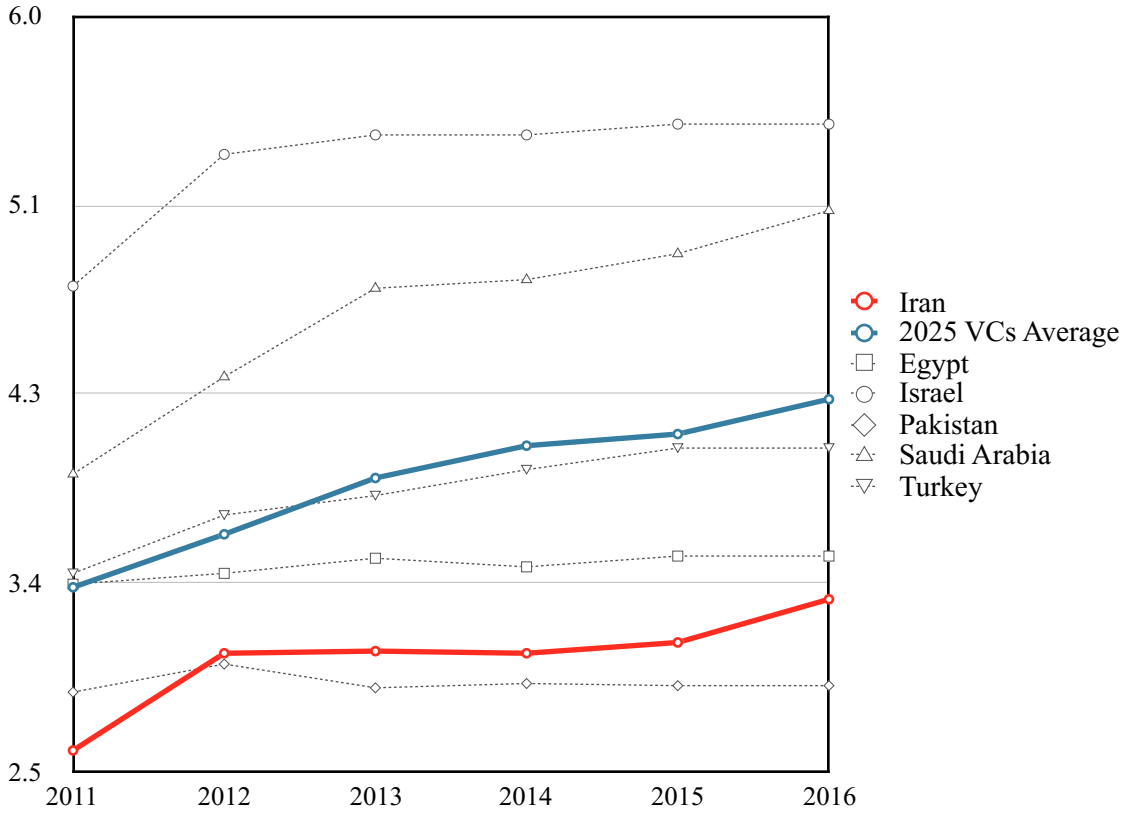


Figure 4.3.3 shows that, except for Pakistan, the usage sub-index value of all sample countries have increased between 2011 and 2016, with Saudi Arabia seeing the highest rate of growth. Among the sample countries the IRI was the lowest ranked in 2011 and since 2012 the second lowest ranked after Pakistan. The figure also shows that the country has seen growth in this sub-index value only in 2011-2012 under Ahmadinejad and 2015-2016 under Rouhani, and for the rest of the period in question the sub-index value has remained nearly constant.

[360] Ibid.

As Table 4.3.3 illustrates, among the three main components of the sub-index, the business usage value has not significantly changed since 2012. The figure also shows that during the Ahmadinejad administration the government usage value has increased while individual usage declined. This trend was reversed under Rouhani, with government usage declining while individual usage saw a major rise. The lack of progress in the utilization of ICTs by the government for optimizing both its bureaucratic machinery and delivering services to the public meant that a rise in the individual usage did not translate to an overall improvement of the usage sub-index. For the country to have a better performance usage sub-index, it needs to maintain the recent growth trend in individual usage, while at the same time improving the ICT usage by both the business sector and government.

Table 4.3.3: The Usage Sub-index Rankings and Values of the IRI (2012-2016)

Year	2012	2013	2014	2015	2016
Individual Usage Rank	92	108	111	100	90
Individual Usage Value	2.63	2.20	2.39	2.9	3.3
Business Usage Rank	121	119	129	129	126
Business Usage Value	3.00	2.99	3.00	3.0	3.1
Government Usage Rank	92	71	91	109	93
Government Usage Value	3.51	4.00	3.76	3.4	3.5

4.3.4 Impact sub-index

The last sub-index assesses ICTs' broad economic and social impacts. The economic component of the sub-index measures the impact of ICTs on innovation in the economy as measured by the "number of patent applications as well as by the role of ICTs in the development of new

products, processes, and organizational models."[361] The economic component also assesses the country's overall progress towards a knowledge-intensive economy. The second component measures the societal progress brought about or enhanced by the use of ICTs in terms of access to education and healthcare, energy savings, and active civil participation. This social component also gauges the positive impact of ICTs on government efficiency and engaging the citizens in public policymaking processes.

Figure 4.3.4: Impact Sub-index

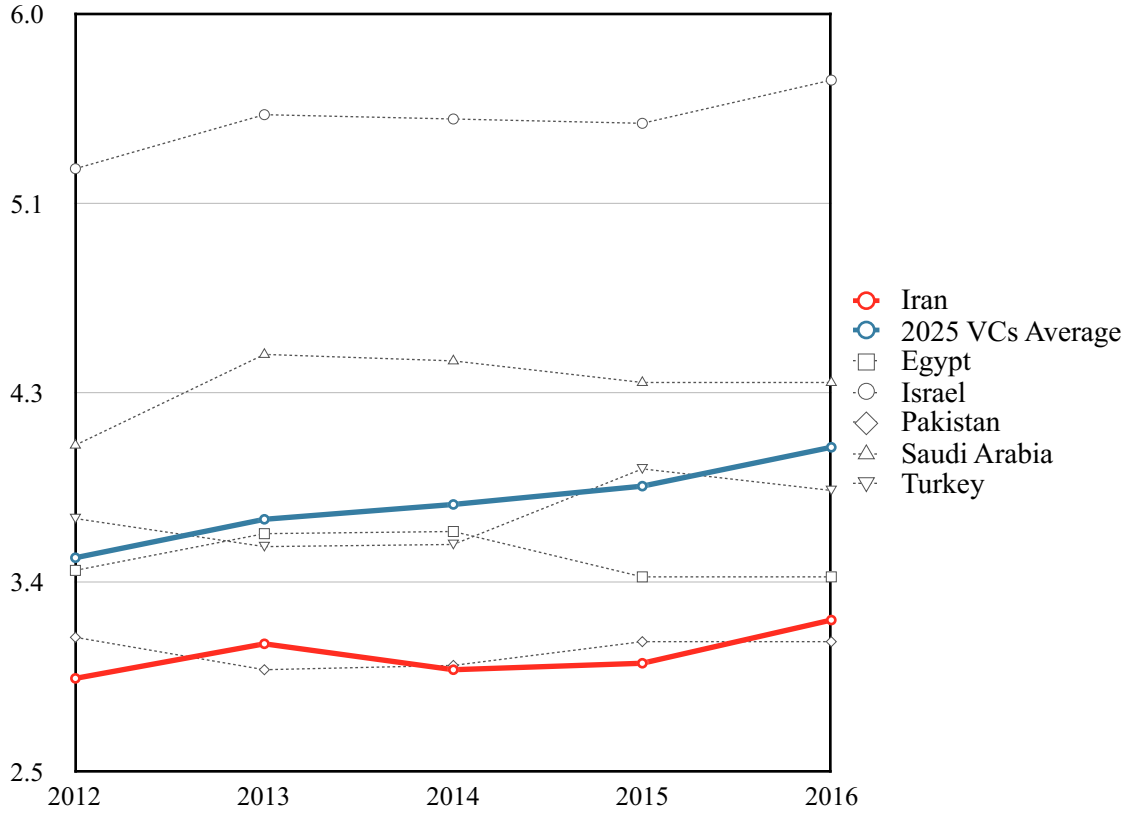


Figure 4.3.4 shows that the 2025 Vision targeted countries' average, along with all the sample countries except Egypt, have experienced growth between 2012 and 2016. Among the sample countries, Israel and Pakistan have the highest and lowest growth rates, respectively. Iran's

[361] Ibid. p.6.

impact sub-index value has been consistently below the 2025 Vision targeted countries' average, and in 2012, 2014, and 2015 the country was the lowest ranked among the sample countries. As Table 4.3.4 shows, although both economic and social components of the index saw growth by the end of the Ahmadinejad administration, this trend was reversed during the first two years of the Rouhani administration. Since 2015, however, the country has experienced growth again in both economic and social components of the sub-index, and if this high rate of growth continues the country will likely improve its standing among the 2025 Vision targeted countries in the next few years. The poor performance of the economic impact sub-index indicates that despite the IRI's emphasis on a shift towards a knowledge-intensive economy, the government has underperformed in terms of supporting research and development institutions as the engines of a knowledge-intensive economy. On the social impact side, the sub-index shows that the government and main economic sectors are unable to utilize ICTs in delivering services to the public, particularly in the education, healthcare, and financial domains. More critically, the government has been quite unsuccessful in the utilization of ICTs to optimize its operational efficiency and engage citizens in the policymaking process.

Table 4.3.4: The Impact Sub-index Rankings and Values of the IRI (2012-2016)

Year	2012	2013	2014	2015	2016
Economic Impacts Rank	107	106	114	110	100
Economic Impacts Value	2.76	2.82	2.77	2.7	2.9
Social Impacts Rank	107	94	105	115	101
Social Impacts Value	3.10	3.36	3.17	3.2	3.5

4.4. ICT Development Index (IDI)

Since 2002, The International Telecommunications Union (ITU) has been publishing the Measuring the Information Society Report to assess the development of ICT and extent of the digital divides between regions and countries over time. The main benchmarking tool used in the reports is the ICT Development Index (IDI) that aggregates quantitative indicators for ICT access, ICT use and ICT skills in more than 150 economies. ICT Development Index reports since 2002 have consistently underlined the strong association between economic and ICT development. In the 2016 IDI ranking, for instance, the average IDI value of Global North countries (7.40) is 82 percent higher than Global South countries (4.07). The 2016 results also show that the bottom 27 countries are all Global South countries, and that the gap in IDI values between Global North and Global South countries is actually widening.[362] ICT Development Index results between 2002 and 2016 show that the IRI's highest rank was 89 out of 175 countries in 2016, and its lowest rank 99 out of 152 countries in 2010 (Table 4.4).

Table 4.4: The ICT Development Rankings of the IRI (2002-2016)

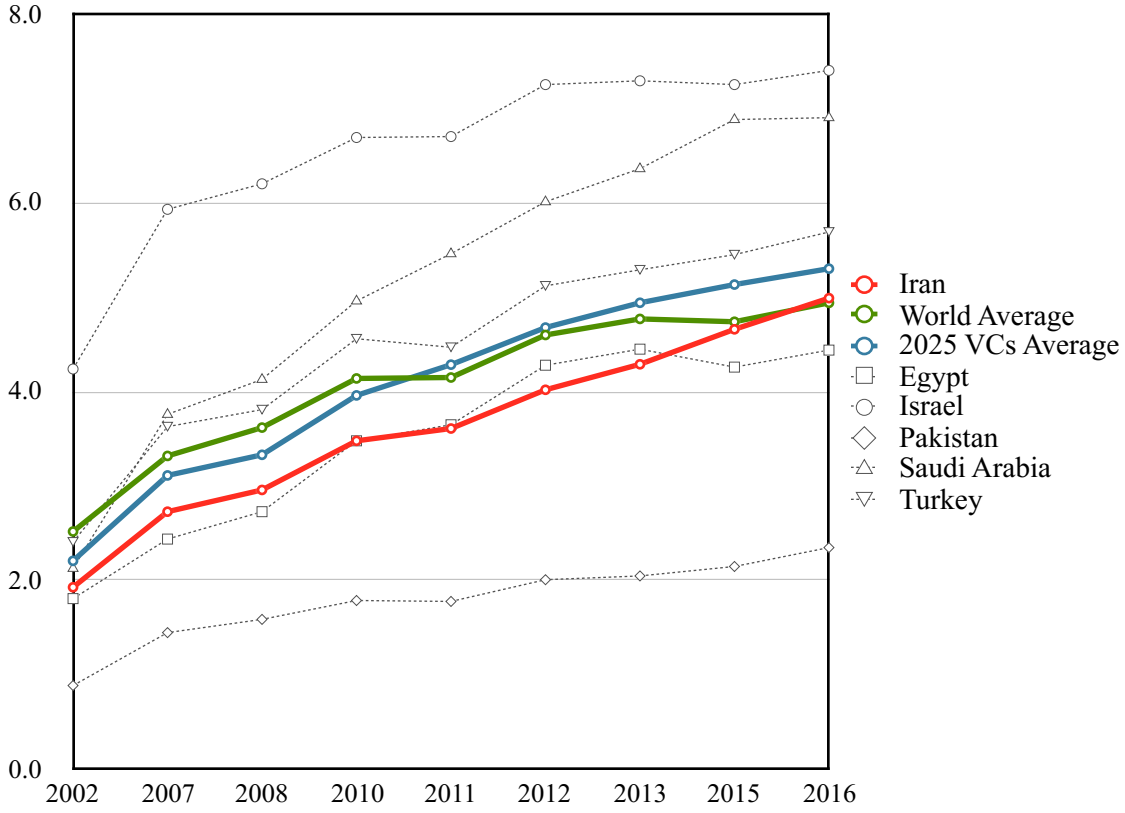
Year	2002	2007	2008	2010	2011	2012	2013	2015	2016
Rank	92	86	84	99	88	97	94	90	89
Total Countries Ranked	154	154	159	152	155	157	166	167	175

Figure 4.4 shows that the IDI values for all the sample countries have increased between 2002 and 2016, with Saudi Arabia and Pakistan having the highest and lowest growth rates,

[362] ITU. "Measuring the Information Society Report 2016." *The International Telecommunication Union (ITU)*. 2016. Web. 01 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf>.

respectively. Like other sample countries, Iran has seen a regular growth rate close to the 2025 Vision targeted countries' average, with almost consistently higher IDI value than Egypt and Pakistan. Israel, Saudi Arabia and Turkey are the only sample countries with the IDI values above the world average during the whole period between 2002 and 2016. Iran's IDI value, in contrast, has been always below both the world and the 2025 Vision targeted countries' average, except in 2016 when the country was able to marginally surpass the world average.

Figure 4.4: ICT Development Index (IDI)



Given this association between ICT and economic development, the Measuring the Information Society reports suggest that in order for countries to exploit the potential of ICTs in enhancing economic growth and development, they must advance through the following three stages: Stage

1: ICT readiness, in which a country achieves a high level of networked infrastructure and access to ICTs; Stage 2: ICT intensity, in which wide ICT use by the public is actualized; and Stage 3: ICT impact, where the positive economic outcome of effective ICT use is realized, thanks to the public's high level of ICT skills. These stages correspond to the three main components of the IDI, respectively: ICT access, use, and skills. These components and the related data will be discussed in the following subsections.

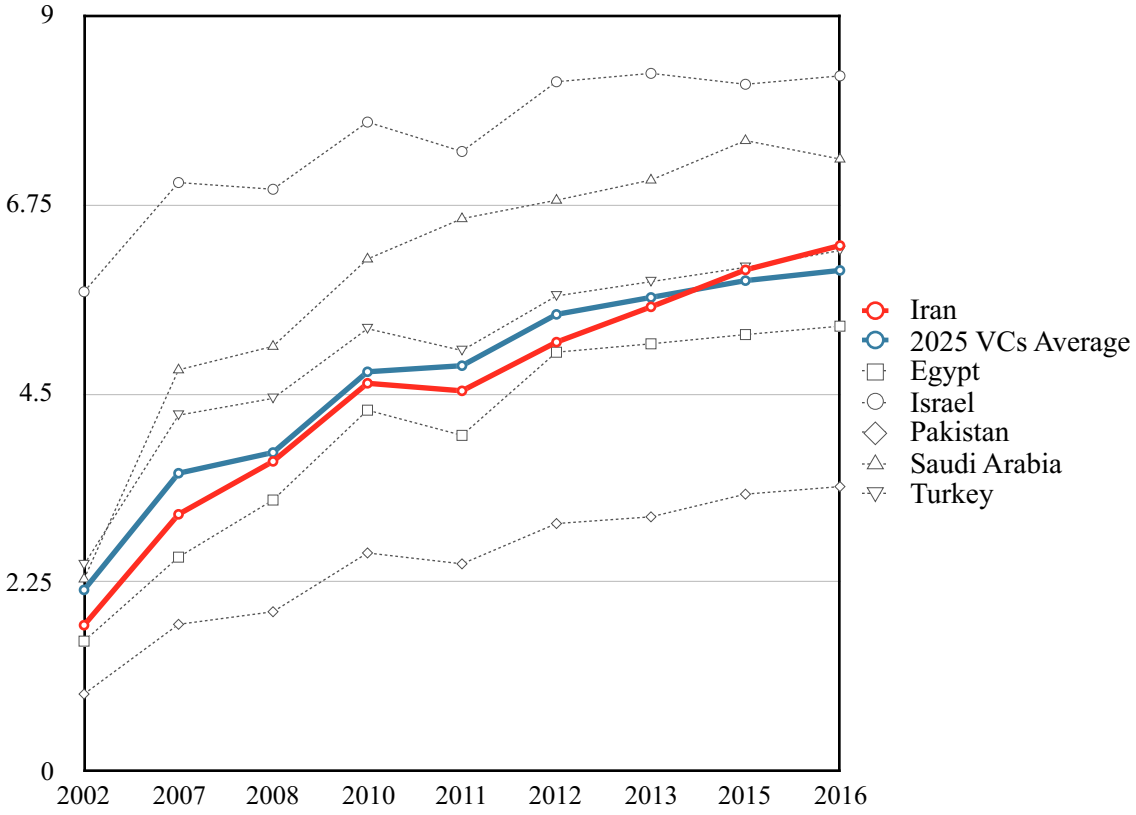
4.4.1 Access sub-index

This sub-index measures ICT readiness through five infrastructure and access indicators: fixed-telephone subscribers per 100 inhabitants; mobile-cellular telephone subscribers per 100 inhabitants; international Internet bandwidth per internet user, which indicates the capacity of a country's network infrastructure for transmitting Internet traffic toward and from other countries; percentage of households with a computer; and percentage of households with Internet access. Figure 4.4.1 shows that the access sub-index values for all the sample countries have increased between 2002 and 2016, with Iran and Saudi Arabia having the highest rates of growth. Iran's Access sub-index value has been consistently above Egypt and Pakistan and, since 2015, above the average of the 2025 Vision targeted countries. The only time period during which country experienced decline in the access sub-index is 2010-2011. This was in large part due to the restrictions put in place by the Ahmadinejad administration on ICT development during the 2009-2010 Green Movement demonstrations, mainly because ICTs were central to the movement's communication strategy.[363] Except for this brief time period, all the three consecutive administrations since 2002 have supported the development of ICT infrastructure,

[363] Safshekan, Roozbeh. "The Matrix of Communication in Social Movements: A Comparison of the 1979 Revolution and 2009 Green Movement in Iran." *Sociology of Islam* 2.3-4 (2014): 328-45.

although the extent of this development still lags behind countries such as Israel and Turkey. Although the main components used in the IDI's access sub-index are different from those used in the EGDI's telecommunications infrastructure and ERI's connectivity and technology infrastructure sub-indexes, since all three are evaluating various aspects of ICT infrastructure development, their results suggest a common growth trend and comparable standing for Iran among the 2025 Vision targeted countries.

Figure 4.4.1: Access Sub-index

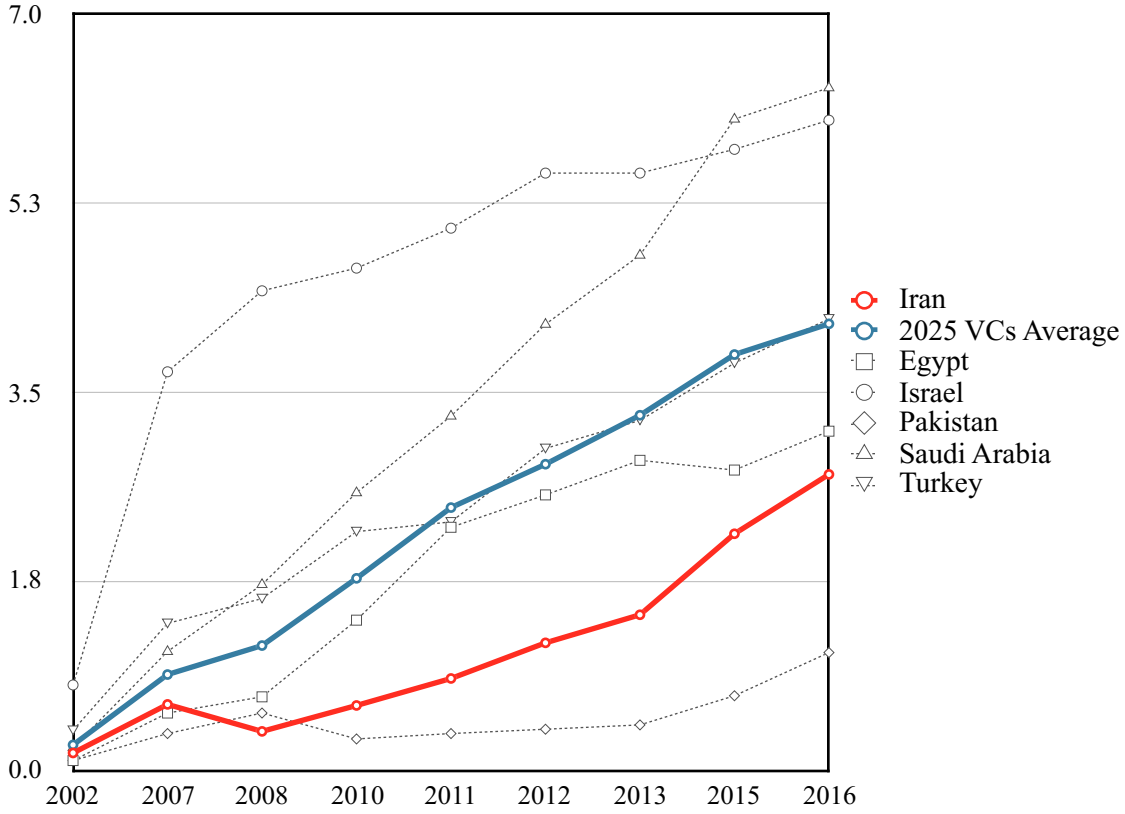


4.4.2. Use sub-index

This sub-index captures the intensity of actual public use of ICTs through the following three indicators: percentage of individuals using the Internet; fixed-broadband subscriptions per 100

inhabitants; and active mobile-broadband subscriptions per 100 inhabitants. The use sub-index values between 2002 and 2016 suggest that all sample countries have experienced growth, with Saudi Arabia and Pakistan seeing the highest and lowest growth rates, respectively (Figure 4.4.2).

Figure 4.4.2: Use sub-index



Israel had been ranked highest among the sample countries for the longest time in this period, but since 2014 Saudi Arabia has held this position thanks to having the highest growth rate among the sample countries. Iran's use sub-index value has been consistently below the 2025 Vision targeted countries's average and, since 2010, it has been the second lowest ranked country among the sample countries, with only Pakistan ranking lower. Among the three sub-indexes of the IDI, this sub-index shows the widest gap between Iran and the 2025 Vision targeted

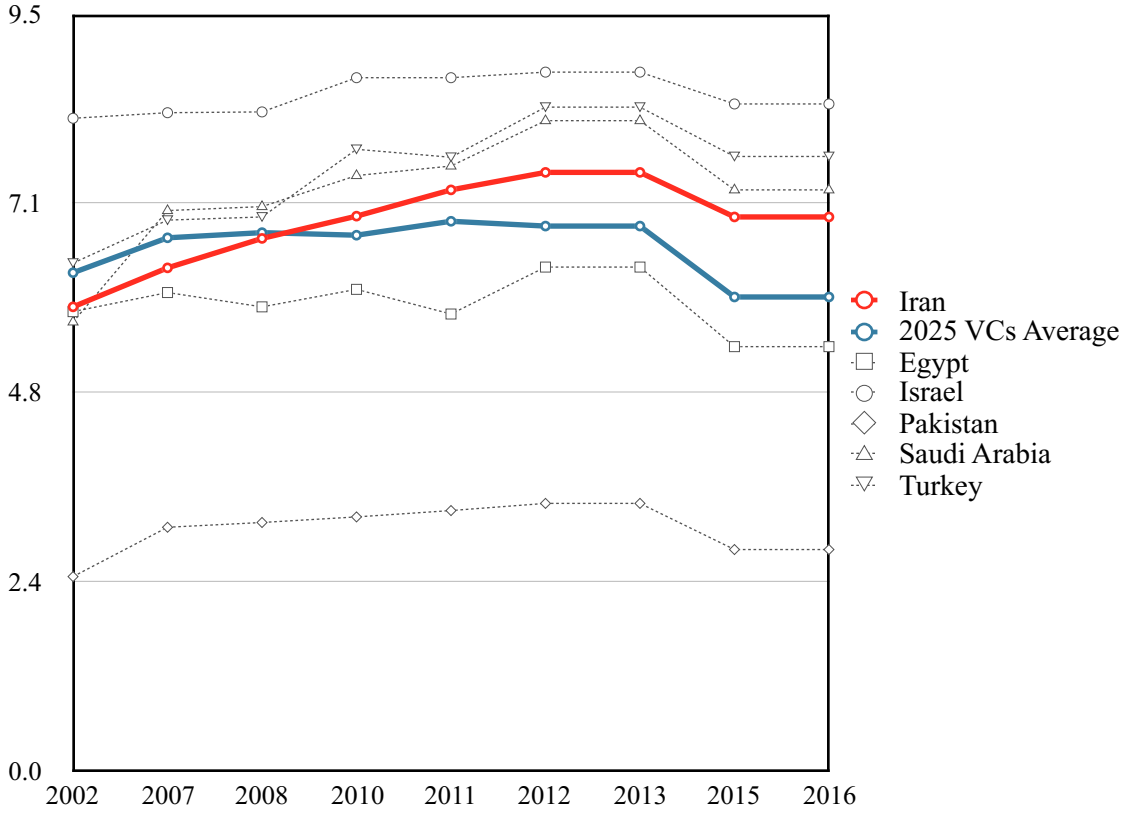
countries' average value. The use sub index-value shows that the country experienced the highest to lowest rates of growth under Rouhani, Khatami and Ahmadinejad administrations, respectively. The only time period during which the use sub index-value declined was 2007-2008, during the first term of the Ahmadinejad administration, as a result of the intensification of the filtering regime in the country. If the high growth rate since 2013 continues, the country will likely surpass the 2025 Vision targeted countries' average in the next few years.

4.4.3 Skills sub-index

This sub-index assesses capabilities or skills required for effective use of ICTs. It includes the following three proxy indicators: mean years of schooling; secondary education gross enrollment ratio; and tertiary education gross enrollment ratio. Figure 4.4.3 shows that Egypt's sub-index value and the 2025 Vision targeted countries's average have declined between 2002 and 2016 while all other sample countries experienced growth, with Turkey and Saudi Arabia having the fastest growth rates. Israel is the top country among the sample countries, while Pakistan is at the bottom with a huge gap with the 2025 Vision targeted countries' average. Among the sample countries, Iran's Skills sub-index value has consistently been higher than Pakistan and Egypt and, since 2010, it has scored above the 2025 Vision targeted countries's average.

Among Iran's IDI sub-indexes, the skills sub-index has the highest value, indicating the high level of education and cyber literacy in the country. Since the IDI's skills sub-index and the previously discussed EGDI's human capital and ERI's social and cultural environment sub-indexes share public education level as an indicator, their corresponding results suggest that Iranians' high level of education and Internet skills are the most pertinent factor in the country's ICT development.

Figure 4.4.3: Skills Sub-index

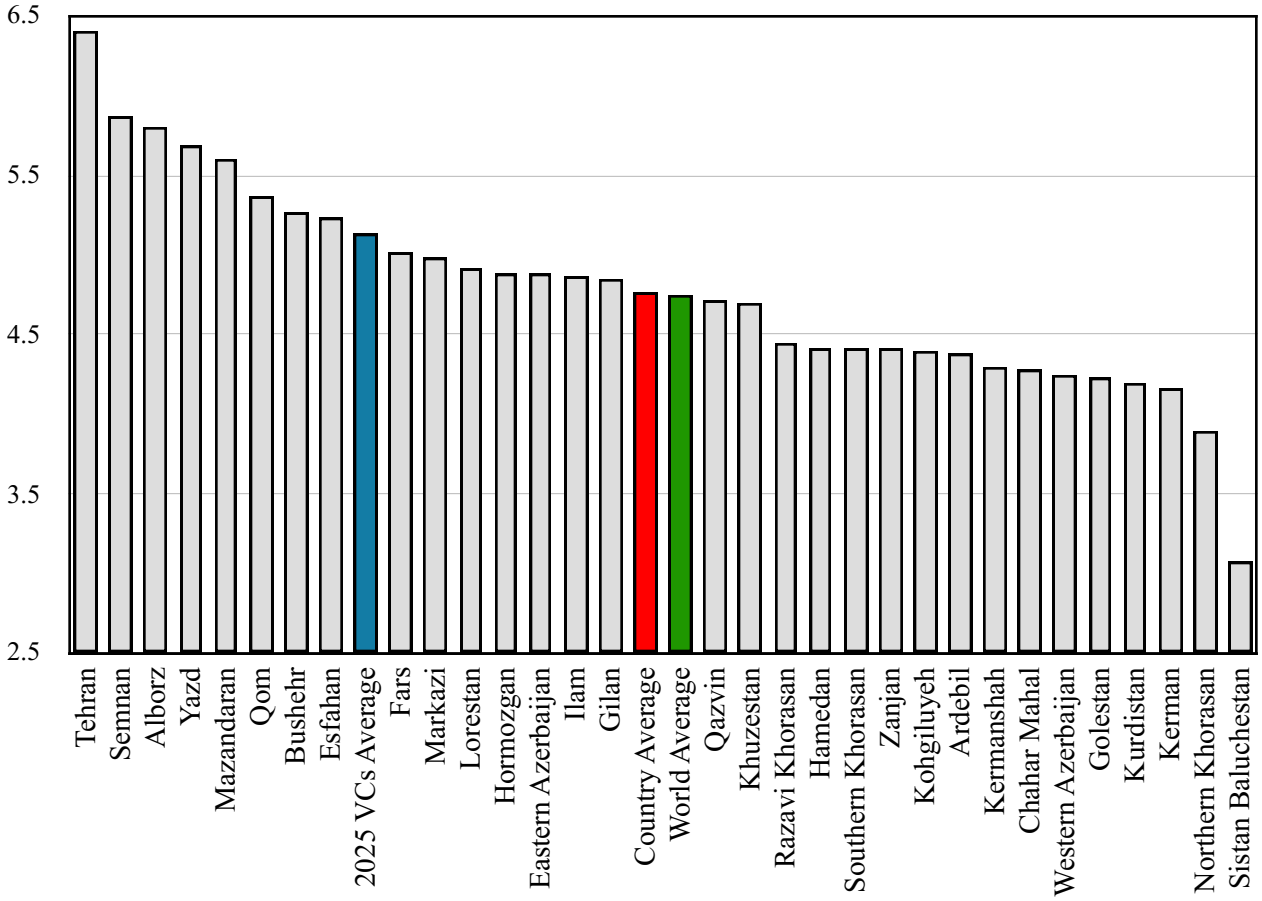


4.4.4 IDI and the digital divide within the IRI

Among the four indexes discussed in this chapter, IDI is the only index for which there is available data from the IRI's 31 provinces. The same methodology used by the ITU in the Measuring the Information Society Reports is incorporated by the Iranian Ministry of Information and Communications Technology (MICT) to assess the level of ICT development in the country's provinces and the extent of digital divides between them. The 2015 MICT results show that Tehran is the most developed province in the country with an IDI value of 6.398, which is still behind the IDI value of 53 countries in the world, including the following 2025 Vision targeted countries: Israel (7.25), United Arab Emirates (6.96), Saudi Arabia (6.88), Qatar

(6.78), Kazakhstan (6.42) and Kuwait (6.45).[364] On the other end of the spectrum, Sistan Baluchestan province is the least ICT developed province in the country with an IDI value of 3.078, only coming above the bottom 51 countries, including: Pakistan (2.15), Afghanistan (1.62), and Yemen (1.96).

Figure 4.4.4: 2015 Provincial IDI Values



As figure 4.4.4 demonstrates, among the 31 provinces of the country, 23 have IDI values lower than the 2025 Vision targeted countries' average, while only Tehran, Semnan, Alborz, Yazd,

[364] MISI. "Vaziat-e Tose-ye Fanavari-ye Ettela'at Va Ertebatat Keshvar (The Country's State of Information and Communication Technology Development)." *The Official Portal of Measuring Information Society of Iran*. Ministry of Information and Communications Technology of Iran, 2015. Web. 01 Mar. 2017. <http://mis.ito.gov.ir/documents/20182/34805/ict94/63cb5ef2-982e-4fbc-9c81-120a0a83e765>.

Mazandaran, Qom, Bushehr, and Esfahan surpass the average. As figure 4.4.4 shows, there is also a significant digital divide between the highest and lowest ICT developed provinces. The average IDI value of the top five provinces (5.9) is almost 50 percent higher than the bottom five provinces (3.9). This discrepancy between the highest (Tehran) and lowest (Sistan Baluchestan) ICT developed provinces is more than 100 percent. Comparing three of the indicators used in the ICT Development Index can help us to better understand the extent of this digital divide. While in Tehran the percentages of households with access to the Internet and computers are 60.7 and 67.7 percent, respectively, these figures for Sistan Baluchestan are 22.4 and 26.1 percent. In Tehran province 54 percent of the population is subscribed to broadband Internet, while this figure for Sistan Baluchestan province is only 11 percent.

Conclusion

The economy is one of the major sources of power for actors in global politics, and cyberspace can impact the power relations between them by providing a new domain for economic activities and competition. In the 2025 Horizon Vision Document, the IRI aimed to become the leading state among the 25 countries in its immediate orbit in the areas of the economy, science, and technology in order to shift the regional balance of economic power in its favor. Developing information and communication technologies and exploiting their huge economic potential have been integral parts of the IRI's efforts to achieve this goal since the ratification of the 2025 Horizon document in 2003. Analyzing the four main indexes of ICT development, this chapter assessed different aspects of ICT development in Iran, the country's standing among the 2025 Vision targeted countries, and its strengths and weaknesses in exploiting the potential of ICTs to

enhance economic growth and development. Our analysis showed that the state of ICT development in the IRI, based on all four indexes, is below both the world and 2025 Vision targeted countries' average. Among the sample countries discussed in this chapter the IRI, along with Egypt and Pakistan, have been consistently lagging behind Israel, Turkey, and Saudi Arabia in many indexes and their respective sub indexes.

The analysis in this chapter showed that the IRI has been close to the average of the 2025 Vision targeted countries in terms of ICT infrastructure development. Iran's ICT infrastructure has continually developed since the early 2000s, with the exception of 2010-2011 period when the Ahmadinejad administration imposed restrictions on ICT development during the Green Movement demonstrations. ICTs played a central role in the communication strategy of the Green Movement by helping mobilize demonstrators and transmit their message around the world. The Green Movement caused considerable alarm within the IRI, which sought to counter it through restrictions which stunted ICT infrastructure development during this period. Since this low point, one of the significant aspect of ICT development under the Rouhani administration has been optimization of the infrastructure in order to reduce the cost of ICT services, manifested in the country's high affordability of ICT services scores. Even this relatively satisfactory level of ICT infrastructure development, however, has translated to a stagnant level of effective utilization of ICTs in economic activities by citizens, business sector, and government.

The IRI's rates of both general and cyber literacy are high, and the citizens have acquired the proficiency of skills necessary for the utilization of novel cyber technologies. Iranians have

developed this level of skill independent of (and in some cases despite) the efforts of their government for two primary reasons. First, cyberspace has offered them a wide range of opportunities and advantages for both personal and professional use, for instance through access to educational material in the form of massive open online courses (MOOCs) and more efficient communication in a work setting. Second, the relatively closed media space in Iran has meant that cyberspace remains as the main domain in which individuals have managed to find freedom of expression and access to information in a relatively unrestricted fashion. Regardless of the high level of skills among citizens, however, the extensive filtering and censorship regime that exists in Iran, backed up by a restrictive penal code for cyber activities, has impeded the full and effective utilization of cyberspace by individuals.

The Iranian business sector faces yet other obstacles in attempting to use ICTs and benefit from their economic potentials. The domestic economic mismanagement and the confrontational foreign policy of the Ahmadinejad administration had a severely negative impact on all sectors of the economy, including the ones related to Internet economy. More broadly, the business sector has faced major obstacles in effectively utilizing ICTs in its economic activities, including excessive bureaucratic red-tape, which has impeded business registration, a dearth of effective laws for regulating online business, and restrictive laws dealing with content generation and communication in cyberspace. The government's lack of support for the business sector research and development (R&D) is yet another barrier in terms of the business sector's utilization and production of innovative technologies and progress towards knowledge-intensive economy. However, not all of these shortcomings can be attributed to government policies (or lack thereof). Iran's relative isolation from the global economic system, as a result of sanctions, has

severely constrained the flow of capital, goods, and technology to Iran, stymieing ICT development.[365]

The government has also experienced difficulties in using ICTs to advance e-government development in Iran. The latter can help streamline and optimize the state bureaucracy, making government processes more efficient and cutting the cost of specific services provided by the government to the public. In Iran, however, where governmental organizations have actually sought to deploy ICTs to increase efficiency and reduce the cost of services, poor website design and slow Internet access speeds have impeded the effective utilization of ICTs by the public to access government information and services. E-consultation and e-decision-making, just two mechanisms for incorporating public opinion into government decision making, can also be utilized to better articulate and implement laws. However, government organization websites in Iran are rarely equipped with online tools, such as social media, online polls, and discussion forums, to consult with the citizenry on public issues and foster public participation in the policy making processes. Finally, even where e-government, e-consultation, and e-decision-making have been implemented in the country to varying degrees, the digital divide in the country between developed versus underdeveloped regions has troubling implications. The stark digital divide that exists between Tehran and Sistan and Baluchestan provinces, for example, means that the former, by virtue of its better access and mastery of cyberspace, will be much better represented when compared to the latter if and when e-government, e-consultation, and e-decision-making initiatives are implemented.

---

[365] Amir Rashidi, interview by author.

In the 2025 Horizon Vision Document the IRI has set forth an ambitious agenda that would see Iran become the leading economic and technology power among a group of 25 countries, including many of its regional rivals. Yet for all of the lofty aspirations laid out in the 2025 Vision document, actual progress in terms of exploiting ICTs for economic growth and development has been limited, uneven, and halting.

CHAPTER FIVE: IRAN AND THE GLOBAL POLITICS OF INTERNET GOVERNANCE

Introduction

As discussed in the literature review and theoretical framework chapters, the decision-making and agenda setting embedded in international institutions constitute one of the main aspects of exercise of power in global politics. International institutions have emerged as important actors on the global stage to promote the rule of law and create organizations and norms, thereby mitigating the conflictual nature of global politics and fostering cooperation among states. Cyberspace, due to its inherently international architecture, has spawned new international institutions of Internet Governance where state and non-state actors engage each other to advance their respective interests. This chapter draws on the trajectory of the Internet Governance agenda pursued by the IRI, showing how it has been shaped and transformed by the interplay of state-society and international relations. Analyzing the official documents of six major global events on Internet Governance since 2003, the chapter illustrates that the IRI agenda of Internet Governance has been preoccupied with three major issues: first, the digital divide and the significant potential of the Internet for economic development; second, the dominant role of Global North countries, particularly the United States, in the management of the critical Internet resources through organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN); and third, the role of non-state actors, such as the private sector and civil society organizations (CSOs), in Internet Governance. The latter issue constitutes the main area of contention between different Iranian presidential administrations. The IRI's state-

centric agenda for Internet Governance under Mahmoud Ahmadinejad's administration (2005-2013) sought to severely limit the role of non-governmental organizations (NGOs) in order to enhance the hegemony of the state vis-à-vis Iranian society. During the Mohammad Khatami and Hassan Rouhani presidencies (1997-2005 and 2013-present respectively), however, the IRI agenda acknowledged the role of non-state actors and was more open to the multi-stakeholder framework of Internet Governance. The chapter concludes that although the aforementioned issues deserve serious attention, overemphasizing them led the IRI to ignore the complexity of the emerging regime of global Internet Governance and, consequently, to overlook pervasive issues such as transnational cybercrime.

This chapter studies the Internet Governance agenda pursued by the IRI at a range of global Internet Governance since 2003 through the following method. First, all of the available documents pertaining to the IRI's involvement in global events on Internet Governance were collected and analyzed. Second, in cases when IRI delegates to these global events referred to the contribution of other parties, the documents of these parties were also analyzed. Third, event outcome documents were assessed to understand the extent to which the IRI's views were reflected in them. The data collected through the above three steps was then evaluated in the context of Iranian domestic politics and foreign policy to determine the main drivers behind the IRI's approach to global Internet Governance. From this universe of events on global Internet Governance since 2003, six were selected for inclusion and deeper study in this chapter. These selected events were the most consistent in terms of containing data for all three steps of data collection laid out above. Additionally, these events best encapsulated the central planks of the IRI's Internet Governance agenda which were also reflected at other events.

5.1. The World Summit on the Information Society: Geneva Phase

The first global venue where discussions around Internet Governance were held was the World Summit on the Information Society (WSIS). Realizing the significance of the emerging global regime of Internet Governance, a high ranking Iranian delegation headed by president Mohammad Khatami participated in the first phase of the WSIS summit in December 2003 in Geneva. During his speech at the summit, Khatami presented a multifaceted agenda which highlighted the IRI's major priorities and concerns about Internet Governance. He identified cyberspace as an ideal domain for the realization of the concept of a "dialogue among civilizations", first proposed by him at the United Nations General Assembly in 1998 as a response to Samuel Huntington's concept of the "Clash of Civilizations".[366] Khatami declared that:

> The entry to the information society is a new opportunity for the entire world population. The "information age" is the "age of dialogue" and the "networked society" is the organizer of the "networked order". We must seek a solution and work out a formula so that "exchange of information" in the information society leads to "dialogue" and shortened distances. At the outset of this millennium, I raised the need for "dialogue among civilizations", in the age of cyberspace, too, we should continue to encourage and promote "dialogue among civilizations".[367]

Khatami's 'dialogue among civilisations' effort came and was in part driven by Iran's increased isolation vis-a-vis the West in the months preceding his election to the presidency. While U.S.-Iran relations had been severed in the aftermath of the 1979-1980 Tehran hostage crisis, they were further exacerbated in August 1996 by the Iran-Libya Sanctions Act which placed great

---

[366] Lynch, Marc. "The Dialogue of Civilisations and International Public Spheres." *Millennium: Journal of International Studies* 29.2 (2000): 307-30.

[367] Khatami, Mohammad. "Statement by H. E. Mr. Mohammad Khatami President of the Islamic Republic of Iran before the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 10 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/geneva/coverage/archive.asp?lang=en&c_type=pl%7C&c_num=1>.

pressure on the Iranian economy by preventing foreign companies from investing more than a token amount in Iran's petroleum sector.[368] This was preceded by a German court ruling in April 1997 which determined that Iran had been responsible for the 1992 political assassination of Iranian-Kurdish dissidents at Mykonos restaurant in Berlin. This led to a coordinated departure of European ambassadors from Tehran, further isolating Iran on the eve of Khatami's election.[369] The newly elected Khatami was determined to end this isolation through a "foreign policy of reintegration" with the West.[370] The crux of this new foreign policy was the emphasis on "the need for cooperation, dialogue and positive understanding among cultures and religions while rejecting the ideology of confrontation which creates mistrust and diminishes the grounds for cooperation among nations".[371] Khatami saw media in general and cyberspace in particular as a key medium for conducting public diplomacy by connecting nations whose governments maintained hostile relationships. Khatami believed that interconnection between ostensibly hostile nations in the cyber age could influence the sectors of society which constituted the base for hostile policies, percolate to the level of political elites, and ultimately reduce or end tensions.

Khatami's agenda at the summit called for cultural diversity in cyberspace, believing that equal opportunities for all cultural, social and linguistic groups would be a significant requirement for establishing constructive dialogue among nations. The summit documents show that the call for cultural diversity was a common theme among a number of delegations who were concerned

---

[368] ILSA. "The Iran-Libya Sanctions Act (ILSA)." *The U.S. Government Publishing Office (GPO)*. 05 Aug. 1996. Web. 01 Oct. 2017. <https://www.gpo.gov/fdsys/pkg/STATUTE-110/pdf/STATUTE-110-Pg1541.pdf>.

[369] Sabet-Saeidi, Shahriar. "Iranian–European Relations: A Strategic Partnership?" *Iran's Foreign Policy: From Khatami to Ahmadinejad*. Ed. Anoushirvan Ehteshami and Mahjoob Zweiri. Berkshire: Ithaca, 2012. 55-72.

[370] Ansari, Ali. *Iran, Islam and Democracy: the Politics of Managing Change*. London: Chatham House, 2006.

[371] Ramazani, R. K. "The Shifting Premise of Iran's Foreign Policy: Towards a Democratic Peace?" *Middle East Journal* 52.2 (1998): 177-87. p.184.

with the possibility that cyberspace could become an instrument of Western cultural and linguistic hegemony. Among these countries was Brazil, whose representative at the first meeting of the Preparatory Committee (PrepCom-1) of the summit called for "Protecting cultural diversity from the homogenizing effect of ICT driven globalization."[372] This concern was not merely restricted to state actors. In their declaration to WSIS, civil society organizations also warned that: "ICT development has too often reinforced inequalities, such as dominance of roman letter based languages (especially English) and marginalization of local, regional and minority languages. Priority should be given in ICT research and development to overcoming barriers and addressing inequalities between languages and cultures."[373] Beside preserving cultural heritage, this issue deserves serious attention because the lack of cultural and linguistic diversity online could also translate to greater disengagement by the peoples of Global South countries with cyberspace, thereby further reducing the extent to which the economic potential of cyberspace for development could be realized.

Another major concern raised in Khatami's agenda and shared by many other representatives was over the "inequalities in the development of infrastructures and global access to and use of information and communication technology", better known as the digital divide.[374] As discussed

---

[372] WSIS. "I PrepCom for the World Summit on Information Society: Statement from Brazil." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 05 July 2002. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing-all-pc.asp?lang=en&c_event=pc|1>.

[373] WSIS. "Shaping Information Societies for Human Needs: Civil Society Declaration to the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 08 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en?&id=1179|1208>.

[374] Khatami, Mohammad. "Statement by H. E. Mr. Mohammad Khatami President of the Islamic Republic of Iran before the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 10 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/geneva/coverage/archive.asp?lang=en&c_type=pl%7C&c_num=1>.

in the literature review, two major analytical approaches to the digital divide can be identified in the academic literature. The first approach defines the digital divide mainly on the basis of access to Information and Communication Technologies (ICTs), thereby equating access with actual use of ICTs, and assumes that all people online have the same ability to use and benefit from these technologies. The second approach highlights different economic and social factors as causing the digital divide through their impact on the use of ICTs, including income, race, gender, geography, culture, education, and technical skills, among other factors. The emphasis on both access to and use of ICTs made the IRI's agenda multifaceted and therefore more compatible with the second approach. The digital divide became a major theme of the summit since many Global South countries view cyberspace as having a significant potential for economic development and reducing the gap with Global North countries. In fact, the decision to hold the WSIS was initially made at the 1998 Minneapolis Conference of the International Telecommunication Union (ITU) to achieve an international consensus on the use of ICTs to fulfill the UN Millennium Development Goals (Table 5.1).

Table 5.1: The United Nations Millennium Development Goals (MDGs)

1. ERADICATE EXTREME POVERTY AND HUNGER	2. ACHIEVE UNIVERSAL PRIMARY EDUCATION	3. PROMOTE GENDER EQUALITY AND EMPOWER WOMEN	4. REDUCE CHILD MORTALITY
5. IMPROVE MATERNAL HEALTH	6. COMBAT HIV/ AIDS, MALARIA AND OTHER DISEASES	7. ENSURE ENVIRONMENTAL SUSTAINABILITY	8. DEVELOP A GLOBAL PARTNERSHIP FOR DEVELOPMENT

The United Nations Conference on Trade and Development (UNCTAD) report on the digital divide showed a huge gap between Global North and Global South countries. According to the 2002 UNCTAD ranking of 165 countries, the top 25 countries in terms of ICT diffusion were all among Global North countries while countries like Brazil, Iran, China, and India, were ranked 57, 84, 118, 121, respectively.[375] The Global South countries emphasized that the equal distribution of ICTs among nations is the main requirement for fulfilling of the MDGs and in the absence of equal opportunities, cyberspace could become a new factor in deepening the gap between the developing and developed worlds. In their submission to the summit, CSOs also shared these concerns, asking the summit to treat the digital divide as a serious issue:

> The unequal distribution of ICTs and the lack of information access for a large majority of the world's population, often referred to as the digital divide, is in fact a mapping of new asymmetries onto the existing grid of social divides. These include the divide between the North and South, rich and poor, men and women, urban and rural populations, those with access to information and those without. Such disparities are found not only between different cultures, but also within national borders. The international community must exercise its collective power to ensure action on the part of individual states in order to bridge domestic digital divides.[376]

On the subject of freedom of expression and access to information in cyberspace, Khatami put a great emphasis on the commitment of states to human rights and principles of democracy. He even went beyond the ideals championed in the Universal Declaration of Human Rights and proposed three new human rights in cyber era: the “right to development”, “right to

---

[375] UNCTD. "The Digital Divide: ICT Development Indices 2004." *United Nations Conference on Trade and Development*, 2004. Web. 10 Dec. 2016. <http://unctad.org/en/docs/iteipc20054_en.pdf>.

[376] WSIS. "Shaping Information Societies for Human Needs: Civil Society Declaration to the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 8 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en?&id=1179|1208>.

communication", and "right to information."[377] Khatami's advocacy for freedom of expression and access to information in cyberspace can be better understood by taking into account the context of domestic politics at the time. During Khatami's presidency the state media was under the tight control of his conservative political opponents, the principlists. This state of affairs led proponents of the Khatami administration in the media to take their message to print in a blossoming of newspapers known as the Press Spring. The raucous reformist press, which engaged in rich if contentious debate over a wide range of issues, soon became a target of principlist suppression, with sixteen reformist outlets shut down by the judiciary in one incident alone in May 2000.[378] In the absence of the ability to convey its message through state media and major outlets, the Khatami administration realized that cyberspace could be a powerful medium for disseminating the platform of the reformist movement to the public, and that preserving freedom of expression in this domain was the only way to break the media restrictions imposed by conservative opponents.[379]

Despite Khatami's overall approach, the Iranian delegation's suggestions on the summit's Declaration of Principles also proposed that freedom of expression in cyberspace needed to be subject to the restrictions provided by Article 29 of the Universal Declaration of Human Rights and by Article 19 and Article 20 of the International Covenant on Civil and Political Rights that prohibit "any propaganda for war" and "advocacy of national, racial or religious hatred that

---

[377] Khatami, Mohammad. "Statement by H. E. Mr. Mohammad Khatami President of the Islamic Republic of Iran before the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 10 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/geneva/coverage/archive.asp?lang=en&c_type=pl%7C&c_num=1>.

[378] Shahidi, Hossein. *Journalism in Iran from Mission to Profession*. London: Routledge, 2010. p.68.

[379] Michaelsen, Marcus. "The Politics of Online Journalism in Iran." *Social Media in Iran: Politics and Society after 2009*. Ed. David M. Faris and Babak Rahimi. Albany, NY: State U of New York, 2015. 101-22. p.105-106.

constitutes incitement to discrimination, hostility or violence."[380] According to these articles freedom of speech can also be subject to certain restrictions for respect of the rights or reputations of others and the protection of national security or public order, health and morals. While Article 29 of the declaration can be said to have been taken into account in the summit and final text of the summit's Declaration of Principles because of the declaration's overall inclusion, the same cannot be said of Articles 19 and 20 of covenant because the latter document was excluded altogether.

The last major theme in Iran's agenda at the Geneva phase of WSIS was the management of critical Internet resources. Khatami's speech, as well as the submission of the Iranian delegation to the summit, highlighted the concerns and priorities of the IRI regarding this issue. In his speech at the summit, Khatami exclaimed that "no government will have the right to impose unilateral decisions, depriving other nations from their rights including correct access to information."[381] He further emphasized that "Global management of internet should find a democratic and comprehensive mechanism to enable all players, including the developing countries, to play an effective role in this arena". It appears that in these remarks, Khatami tacitly challenged the unique and unilateral role of the US government in overseeing the Internet Corporation for Assigned Names and Numbers (ICANN). As discussed previously, ICANN is a private not-for-profit organization which manages internet protocol (IP) addresses and the domain name system (DNS). ICANN's physical location inside the jurisdiction of the United

---

[380] WSIS. "Islamic Republic of Iran (WSIS/PC-3/C/0084)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 31 May 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing-all-pc.asp?lang=en&c_event=pc|3>.

[381] Ibid.

States and, more importantly, its mutual agreements with the US Department of Commerce are viewed by many governments as being problematic. Moreover, ICANN is based on a multi-stakeholder model where the private sector and NGOs play a major role, decreasing the influence which states have to shape the policies and practices of this organization. In the summit, Brazil played a leading role in raising this concern and proposed that states were the ultimate legitimate authorities in terms of Internet Governance and, accordingly, an intergovernmental organization would be appropriate to look after Internet policy making.[382] Iran did not share this view. Although the Iranian delegation challenged the unilateral authority of the United States over ICANN, their submissions to the summit did not promote the role of states at the expense of other stakeholders like the private sector and CSOs. As with the championing of the freedom of expression, the preference of multi-stakeholderism over intergovernmental framework could be better understood in the context of Iranian domestic politics. At the time, Khatami sought to support and strengthen Iran's nascent private sector as a the main pillar of his economic and industrial development plans.[383] He simultaneously viewed a vibrant civil society as central to his social and political reforms, declaring that in a society with strong CSOs the government is "the servant of the people and not their master" and citizens "enjoy the right to determine their own destiny, supervise the governance and hold the government accountable".[384]

---

[382] WSIS. "Brazilian Government Contribution (WSIS/PC-3/CONTR/60-E)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 31 May 2003. Web. 10 Dec. 2016. <https://www.itu.int/dms_pub/itu-s/md/03/.../S03-WSISPC3-C-0060!!MSW-E.doc>.

[383] Pesaran, Evaleila. "Resurrecting the Revolution." *Iran's Struggle for Economic Independence: Reform and Counter-reform in the Post-revolutionary Era*. London: Routledge, 2013. 128-60.

[384] Adib-Moghaddam, Arshin. *International Politics of the Persian Gulf: A Cultural Genealogy*. Abingdon: Routledge, 2009. p.86.

The IRI's position on the multi-stakeholder framework of Internet Governance was somewhat in line with that of the United States, European Union, Japan, and Canada, among others. The tension between these countries and those who challenged multi-stakeholderism was clearly reflected in the main document of the first phase of the summit, the Declaration of Principles, also known as the Geneva Principles. The declaration highlighted that the global management of the Internet should be "multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations." However, it also underlined that: "Policy authority for Internet-related public policy issues is the sovereign right of States".[385] While the final declaration still accorded an "important role" to the private sector on a technical level and to civil society on a community level, these roles remained vague and a hierarchic framework for Internet Governance was tacitly proposed, in which states had the preeminent role. Despite this outcome, tensions around this issue continued to persist.

5.2. The World Summit on the Information Society: Tunisia Phase

Cyberspace, as an alternative space in which relatively free media activities had become possible in Iran, had greatly aided Khatami and the reformists in spreading their message and mobilizing their base. For this precise reason, cyberspace became a new target of the principlists towards the end of the Khatami presidency, who sought to restrict it through the judiciary and security forces under their sway. For example, between August 2004 and February 2005, a total of 18 people were arrested for having "acted against the system by working on illegal internet sites", just one

[385] WSIS. "Geneva Declaration of Principles (WSIS-03/GENEVA/DOC/0004)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 12 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>.

symptom of the growing suppression in cyberspace.[386] The election of Ahmadinejad as president in 2005 effectively handed the principlists a powerful new perch, the executive branch, from which to further expand their online crackdown.

The second phase of the World Summit on the Information Society (WSIS) was held in Tunisia in November 2005, almost three months after the principlist Mahmoud Ahmadinejad assumed office as president. Among the first acts of the new administration was the imposition of restrictions on CSOs, including the Iran CSOs Training and Research Center (ICTRC), which had been designated as the WSIS Regional Civil Society Focal Point for the Middle and West Asia region. Indeed just a few weeks after Ahmadinejad's accession to the presidency, his administration prevented the convening of the 2nd Civil Society Regional Forum on the Information Society for the Middle East and West Asia, which was supposed to be held by the ICTRC on 23-25 August 2005 in Kish Island, Iran. Organized in partnership with several accredited international organizations such as the United Nations, World Bank and UNESCO, the forum had been intended to "provide an opportunity for civil society representatives to discuss the WSIS process; network, share and exchange experience and technical know-how on ICT for development; receive much needed training and capacity building in ICT related areas; and draft a statement which could be presented at the WSIS in Tunisia in November [2005]."[387] Despite this incident, Susan Tahmasebi, an Iranian civil society activist, was present at the second phase of the WSIS in Tunisia to speak on behalf of the CSOs in the Middle East and West Asia Region.

---

386 Shahidi, Hossein. *Journalism in Iran from Mission to Profession*. London: Routledge, . 2010. p.107.

387 Tahmasebi, Sussan. "Iranian Civil Society Organizations Training and Research Center." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 17 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/tunis/scripts/archive.asp?lang=en&c_type=2|17&c_num=301>.

In her speech at the summit she gave a brief report on the closure of the Kish Regional CSO Forum by Iranian authorities, asking the WSIS Secretariat to follow-up with the Iranian government to inquire about the incident and urge it to cooperate with Iranian CSOs to organize another regional forum in Iran. This was among the first incidents where an Iranian CSO representative challenged the Iranian government in an official international venue and called for an explanation from the government about the restrictions it imposed over civil society.

Representation of independent and non-governmental CSO's from the Middle East and West Asia region was another major theme highlighted in Tahmasebi's speech. To participate in formal UN deliberations, NGOs need to be accredited by the United Nations Economic and Social Council (ECOSOC). Governments often manipulate the ECOSOC Accreditation process to create government-sponsored CSOs and send them to international venues in the guise of genuine independent NGOs. These pseudo-CSOs in turn help governments to legitimize their agendas within international organizations. Addressing the issue of pseudo-CSOs, Tahmasebi asked for reforms in the ECOSOC Accreditation process and the establishment of "an independent structure, comprised of independent non-governmental CSOs themselves, which would be charged with oversight and administration of ECOSOC accreditation of CSOs."[388] The Civil Society Declaration submitted to the summit also raised the issue of representation of genuine CSOs and asked for: "developing clearer and less bureaucratic rules of recognition for accrediting CSOs in the UN system, for instance in obtaining ECOSOC status and summit accreditation, and to ensure that national governmental recognition of Civil Society entities is not

[388] Ibid.

the basis for official recognition in the UN system."[389] Shirin Ebadi, the 2003 Nobel Peace Laureate and the chairwoman of The Defenders of Human Rights Center in Iran, was another Iranian civil society representative at the summit who shared the concerns of Tahmasebi and other CSO representatives on the issue of representation of CSOs at international forums. Speaking on behalf of International Federation of Human rights, she asserted that authoritarian governments would often manipulate international forums by "stacking them with pseudo-NGOs that they have set up to spread disinformation about the situation" within their countries.[390]

While freedom of expression and access to information were championed in the 2003 Geneva Declaration of Principles and Plan of Action, by the time of the second phase of the summit in 2005, many governments had initiated severe Internet filtering regimes to control the content produced and consumed by their citizens. The rising trend of censorship in cyberspace thus became a major concern of CSOs active in the West Asia and Middle East countries. Speaking on behalf of CSOs in these countries, Tahmasebi asked the summit to address this issue in its deliberations and design a vigorous monitoring mechanism over signatory governments to the Geneva Declaration and Action Plan in order to hold them accountable to their commitments stated in the aforementioned texts. Another policy pursued by some governments in the region was the restriction of freedom of speech and assembly of CSOs advocating free cyberspace and training citizens to use the Internet. Tahmasebi asked the summit to adopt Article 19 of the Universal Declaration of Human Rights as the guiding principle in its deliberations, and

---

[389] WSIS. "Tunis Phase: Civil Society Declaration (WSIS-05/TUNIS/CONTR/13)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 23 Dec. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing-all.asp?lang=en&c_event=s|2&c_type=all|>.

[390] Ebadi, Shirin. "International Federation for Human Rights." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 16 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/tunis/scripts/archive.asp?lang=en&c_type=2|16&c_num=293>.

guarantee free speech and freedom of assembly for CSOs in general, and those working on Internet related advocacy and training in particular.

Like the first phase of the summit in Geneva, the digital divide was among the dominant themes of the summit in Tunisia. Speaking on this issue, Ebadi expounded on how the significant potential of cyberspace for economic and political development goals would be squandered by the deepening digital divide both between and within the nations around the globe. By contrasting military spending with the financial resources required for eliminating the digital divide, she criticized governments for the lack of vision and will to tackle this issue:

> Around the globe, thirty developed countries, making up only 16 per cent of the total world population, spend some USD 750 billion every year on the military budget; compare this with the USD 100 billion that would be needed to lift the undeveloped countries out of IT poverty, and bring their information and communications infrastructure up to a decent level.[391]

The dominant role of Global North countries in the management of the critical Internet resources was also challenged by CSOs present at the summit, with Ebadi being among the chief critics. This dominance, she asserted, would have serious ramification for the people in the Global South since Global North countries could utilize their leverage over Internet infrastructure and deprive Global South countries of internet access if this suited their political and economic interests. A similar logic applied to authoritarian governments, who monopolize the management of critical Internet resources at national level to enhance their hegemony over society. Ebadi explained that these governments frequently use “national security, morality or illegal commerce as an excuse

---

[391] Ebadi, Shirin. "International Federation for Human Rights." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 16 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/tunis/scripts/archive.asp?lang=en&c_type=2|16&c_num=293>.

to selectively block internet content, expose sites to selective filtering, and prevent people from gaining ready access to information that they need, and making themselves heard outside. Even worse, these governments punish bloggers who dare to express the slightest criticism."[392] Challenging the abuse of power over cyberspace by authoritarian governments, she called for the creation of a committee in the United Nations consisting of representatives from the Office of the High Commissioner for Human Rights (OHCHR), United Nations Educational, Scientific and Cultural Organization (UNESCO), United Nations Development Program (UNDP), International Telecommunication Union (ITU), and non-governmental organizations (NGOs), to monitor content filtering regimes imposed by the governments and hold them accountable for respecting the people's right for freedom of expression and access to information in cyberspace.

The World Summit on the Information Society in Tunisia differed from its first iteration in Geneva in a number of substantive ways. For Iran this included representation of Iranian CSOs viewpoints on different aspects of Internet Governance by Tahmasebi and Ebadi. Another major difference between the two phases had to do with the Internet Governance agenda presented by the Iranian government delegation. In a sharp turn, the multi-stakeholder Internet Governance framework presented in the first phase was replaced by a government-centric one in the second summit. This is best evident in the Iranian delegation deliberations in the third Preparatory Committee (PrepCom-3) of the summit in September 2005 where Iran played a leading role in establishing a coalition promoting a new model for global Internet Governance.[393] Iran's model

---

[392] Ibid.

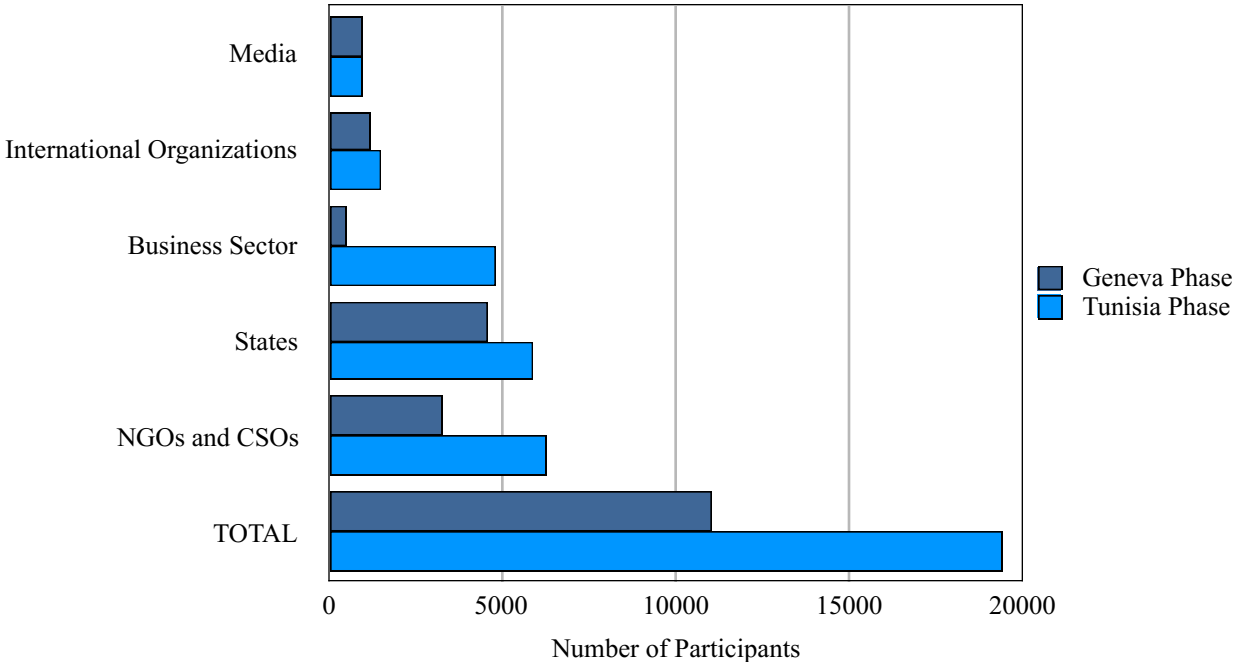
[393] WSIS. "Proposal on Internet Governance Islamic Republic of Iran (WSIS-II/PC-3/DT/22)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 30 Sept. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing.asp?lang=en&c_event=pc2%7C3&c_type=td%7C>.

proposed an intergovernmental Council for Global Public Policy and Oversight in which other stakeholders such as the private sector and CSOs would participate in a purely advisory capacity. The council would be anchored in the United Nations system and take oversight authority over ICANN from the US Department of Commerce. The model also proposed that the council would have authority over several aspects of Internet Governance, including: a) addressing international public policy issues relating to Internet resource management and those not falling in the scope of other existing intergovernmental organizations; b) facilitating negotiations of treaties, conventions and agreements on Internet-related public policy issues; c) fostering and providing guidance on developmental issues including capacity-building, multilingualism, equitable and cost-based international interconnection costs, and equitable access for all; and d) approving rules and procedures for dispute resolution mechanisms and conduct arbitration.

In summary, Iran's proposed Internet Governance model at the Tunisia phase had three main components, namely: a) a new International governing organization; b) full authority of this organization over almost all Internet related public policy issues; and c) a dominant role for governments in the organization at the expense of the private sector and CSOs, whose role would be reduced to a purely advisory role. Suffice it to say that this model did not garner much support even among state actors at the summit. For one thing, it was against WSIS Geneva's spirit of multi-stakeholderism, besides which it would require much of the existing Internet Governance machinery to be renegotiated. For another, it was not feasible, given there were many Internet Governance issues to which non-state actors were crucial. This was due to what Laura DeNardis has called "The Privatization of Internet Governance", which refers to the increasing degree to which private corporations and nongovernmental entities own and manage much of the technical

resources that keeps the Internet operational.[394] The prominence of non-state actors is demonstrated in part by the sharp rise in the number of the business sector and NGOs/CSO representatives in the second phase of the summit in Tunisia versus the first phase in Geneva (Figure 5.1).[395]

Figure 5.1: Number of Participating Stakeholders in WSIS by Type



Non-state actors were skeptical of any model proposing a single government-centric body with authority over all Internet related public policy issues. While several representatives of the private sector and CSOs called for reforming ICANN to eliminate control of the United States over the organization and make it more accountable, transparent, and democratic, almost none of them supported the creation of a new intergovernmental organization with authority over Internet-related public policy issues. Ultimately this was the approach reflected in the main

[394] DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014. p.11-15.

[395] WSIS. "Participation." *World Summit on the Information Society*. The International Telecommunication Union (ITU), Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/participation/index.html>.

outcome document of the WSIS second phase, the Tunis Agenda for the Information Society. The agenda's Paragraph 55 stated: "We recognize that the existing arrangements for Internet Governance have worked effectively to make the Internet the highly robust, dynamic and geographically diverse medium that it is today, with the private sector taking the lead in day-to-day operations, and with innovation and value creation at the edges."[396] Although the agenda never mentioned ICANN by name, by emphasizing the merits of "existing arrangements for Internet Governance", it did reject the need for a new inter-governmental organization that would take over ICANN's functions and let the latter continue to play its role in Internet Governance. At the same time the agenda paved the way for long-term reforms in ICANN by highlighting that "there is a need to initiate, and reinforce, as appropriate, a transparent, democratic, and multilateral process, with the participation of governments, private sector, civil society and international organizations, in their respective roles."[397] In summary, the Tunis agenda proposed that ICANN would continue to play its role in Internet Governance while incorporating changes to reduce the unilateral oversight of the United States over the organization and enhance the role of other stakeholders in its management. However, the overall issue regarding the roles that state and non-state actors should play in Internet Governance was left unresolved and, as a result, the debate over this issue continued to dominate the discussions in the next major Internet Governance events, chief among them the 2012 World Conference on International Telecommunications (WCIT-12) in Dubai.

---

[396] WSIS. "Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6 (rev. 1))." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 18 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>.

[397] Ibid.

5.3. The 2012 World Conference on International Telecommunications (WCIT-12)

In 2006 the International Communication Union (ITU) decided to review the International Telecommunication Regulations (ITRs) and bring them into line with the significant changes that had taken place in information and communication technologies since it had last been updated in 1988. The magnitude of the changes during this time period was illustrated in the fourteen hundred-fold growth in the number of mobile telephone subscriptions worldwide from 4.3 million to over six billion as well as the rise in the number of Internet users from a few dozen to more than 2.5 billion.[398] To catch up with these changes, the ITU called for the ITRs to be updated by the World Conference on International Telecommunications in 2012 (WCIT-12). Two unique aspects of the WCIT-12 made it distinct from international ICT-related forums such as the World Summit on the Information Society. First, the conference, held under the auspices of the ITU, was an inherently intergovernmental venue. Although a number of technical and legal experts and representatives from the private sector and CSOs attended the conference, only government representatives were allowed to participate in discussions and ultimately vote on the conference outcomes. Second, the WCIT-12 was a treaty-level conference meaning that once its provisions were adopted, they would become binding international law on all ITU Member States. This was in stark contrast to the previous multilateral forums on global Internet Governance that had no authority in terms of making binding international law. In the absence of non-state actors in the policy making process at the conference, the ITU member states in favor of a state-centric regime of Internet Governance were now able to advance and ultimately realize

---

[398] ITU. "Transcript of the Plenary 1, WCIT-12." *The International Telecommunication Union (ITU)*. 03 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec3plenary1.docx>.

their vision in the form of international law. In this vein, the delegation of the IRI under the Mahmoud Ahmadinejad administration, which had been quite unsuccessful in pushing forward its agenda during the second phase of the WSIS in 2005, viewed the WCIT-12 as an opportunity to once again promote its vision of a sovereigntist and government-centric regime of global Internet Governance. The Ahmadinejad administration was especially motivated to implement this vision by the experience of the 2009-2010 Green Movement demonstrations that had used cyberspace as a centerpiece of its communication and mobilization strategy thereby posing a political challenge to the government.[399] By managing cyberspace along more government-centric lines, the IRI hoped to preclude such a scenario from taking place in the future. Drawing on the official documents of the conference, this section shows how the IRI delegation played a leading role during the WCIT-12 to expand the role of governments in Internet Governance at the expense of non-government actors.

In the lead-up to the WCIT-12, proponents of the multi-stakeholder model of Internet Governance underlined the intergovernmental and treaty-level nature of the conference, warning that certain member states would take advantage of the WCIT-12 to impose governmental control over the Internet at the expense of human rights. Addressing these concerns at the first plenary session of the conference, Hamadoun Touré, then Secretary General of the ITU, tried to assure the critics that human rights and freedom of expression would not be up for negotiation at the conference.[400] He asserted that Article 33 of the ITU's constitution guaranteed “the right of

---

[399] Safshekan, Roozbeh. "The Matrix of Communication in Social Movements: A Comparison of the 1979 Revolution and 2009 Green Movement in Iran." *Sociology of Islam* 2.3-4 (2014): 328-45.

[400] ITU. "Transcript of the Plenary 1, WCIT-12." *The International Telecommunication Union (ITU)*. 03 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec3plenary1.docx>.

the public to use the international telecommunication service", and that conference outcomes could not contradict this provision.[401] What he did not mention, however, was the right of states to cut off telecommunications, stated in the Article 34 of the ITU constitution. According to this article, ITU Member States have the right to stop transmission and cut off telecommunications "which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."[402] The general secretary's attempts at reassurance that human rights would be protected was not enough for many countries including Tunisia, the pioneer of the Arab Spring, which had experienced the potential of cyberspace for organizing demonstrations as well as government attempts to curtail this potential by cutting of the ICTs during the Jasmine Revolution of 2010. Reflecting on this experience, the Tunisian representative insisted that provisions such as Article 33 of the ITU constitution did not prevent repressive governments from violating human rights in cyberspace and that the protection of these rights must be explicitly stated in the revised ITRs:

> Existing texts haven't prevented some countries cutting off international telecommunications, and that's why we in Tunisia think that this conference should give a very strong signal about the need to protect this right of the Freedom of Expression. We need, I think, to make explicit the fact that this kind of cutting off of international telecommunications is unacceptable.[403]

The Tunisian delegation's concerns were not merely reflective of their country's experience. The Green Movement, which had risen up following allegations of fraud in the 2009 Iranian

---

[401] ITU. "Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference (Edition 2015)." *The International Telecommunication Union (ITU)*. 2015. Web. 10 Dec. 2016. <https://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000155201PDFE.PDF>. p.43.

[402] Ibid.

[403] ITU. "Transcript of the Plenary 2, WCIT-12." *The International Telecommunication Union (ITU)*. 04 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec4plenary2.docx>.

presidential election, had used cyberspace as a centerpiece of its communication and mobilisation strategy, becoming a model for the Arab Spring movements that followed.[404] Given the centrality of cyberspace to the continued functioning of the Green Movement, the IRI used its monopoly over ICTs to cut off the movement's access to cyberspace. In the days and weeks following the election, the number of websites filtered by authorities shot up dramatically, and at least 50 bloggers and online activists were arrested.[405] It is therefore not surprising that the IRI, having dealt with this issue only a short period before, objected to Tunisia's proposal at the WCIT in 2012.

The IRI delegation objected to the Tunisian proposal, asserting that the ITR's must remain focused on technical aspects of ICTs and that the proposal "should not be discussed at this conference and should not be included in the ITR in any part of the Regulations."[406] According to the IRI delegation, for the Tunisian proposal to be approved by member states, the ITU constitutions might need to be amended and thus the proposal would need to be presented at a plenipotentiary conference with authority over amending the ITU constitution. Despite the objections from the IRI, Saudi Arabia, China, and a few other countries, Secretary General Touré fully supported the Tunisian proposal, emphasizing that "It will serve the cause of this conference, to make it clear to the rest of the world that indeed this conference will stand for freedom of speech and will strengthen, in general, universal Human Rights."[407] A majority of

---

[404] Safshekan, Roozbeh. "The Matrix of Communication in Social Movements." *Sociology of Islam* 2.3-4 (2014): 328-45.

[405] Kelly, Sanja, Sarah Cook, and Mai Truong. "Freedom on the Net 2012: A Global Assessment of Internet and Digital Media." *Freedom House*. 24 Sept. 2012. Web. 01 Oct. 2017. <https://freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report_0.pdf>. p.273.

[406] Ibid.

[407] ITU. "Transcript of the Plenary 4, WCIT-12." *The International Telecommunication Union (ITU)*. 07 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec7plenary4.docx>.

delegations embraced the proposal and ultimately the preamble of the ITRs underlined that "Member States affirm their commitment to implement these Regulations in a manner that respects and upholds their human rights obligations."[408]

Besides the protection of human rights, critics of the WCIT-12 warned that the ITU would use the conference to extend its authority over the Internet. Again, this concern was addressed in the speech of Secretary General Touré in the first Plenary session of the conference: "In preparing for this conference, we have seen and heard many comments about ITU or the United Nations trying to take over the Internet. Let me be very clear one more time: WCIT is not about taking over the Internet. And WCIT is not about Internet Governance."[409] Despite this assertion by the ITU's Secretary General, the conference deliberations and outcome moved towards extending the scope of the conference to include Internet Governance issues. The IRI played a leading role in this regard when its representative proposed that the preamble of the ITRs should recognize the right of access of Member States to the Internet and its resources. While agreeing with the principle of non-discriminatory access to ICTs, several countries objected to this proposal on the grounds that issues relating to the Internet fell outside of the scope of the conference. Ultimately, while the ITRs' preamble recognized "the right of access of Member States to international telecommunication services," it did so without making an explicit reference to the Internet and its resources.[410]

---

[408] ITU. "Final Acts of the World Conference on International Telecommunications (WCIT-12)." *The International Telecommunication Union (ITU)*. 2012. Web. 10 Dec. 2016. <https://www.itu.int/pub/S-CONF-WCIT-2012/en>.

[409] ITU. "Transcript of the Plenary 1, WCIT-12." *The International Telecommunication Union (ITU)*. 03 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec3plenary1.docx>.

[410] ITU. "Final Acts of the World Conference on International Telecommunications (WCIT-12)." *The International Telecommunication Union (ITU)*. 2012. Web. 10 Dec. 2016. <https://www.itu.int/pub/S-CONF-WCIT-2012/en>.

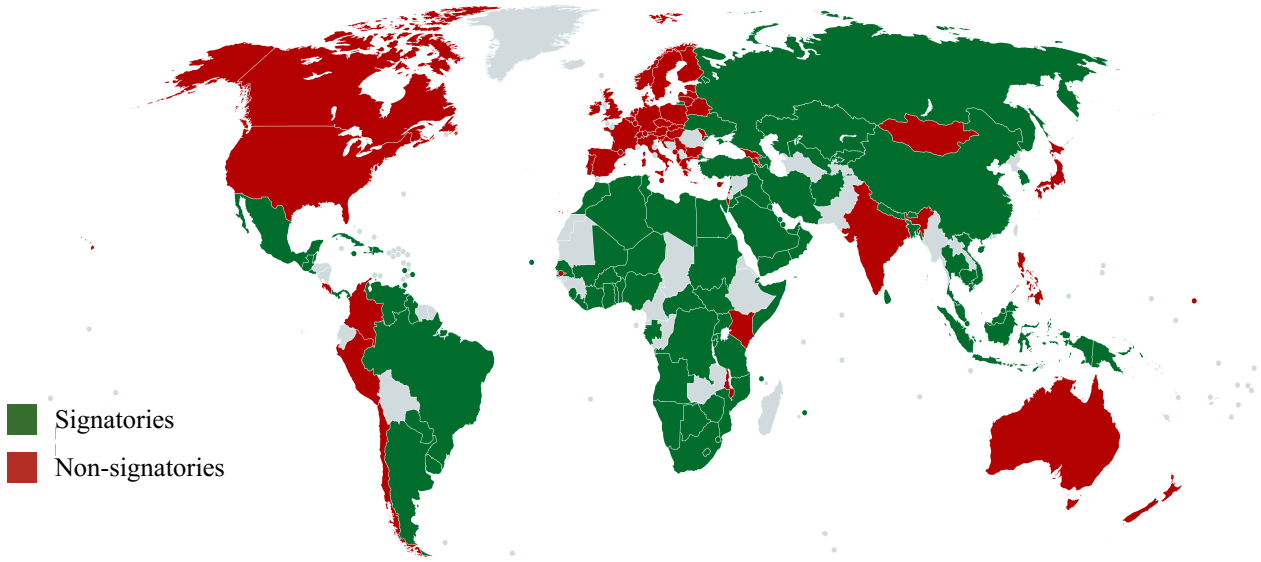
Iran was not the only country attempting to extend the scope of the conference to include Internet related issues. In the third plenary session of the conference Russia argued that the Internet is an inalienable part of the global telecommunications infrastructure and that Internet Governance issues should be included in conference deliberations. The Russian proposal tacitly denied the multi-stakeholder framework of Internet Governance celebrated in the WSIS documents by emphasizing "the rights of Member States of the ITU on issues related to internet governance."[411] China embraced the Russian vision and fiercely supported that idea of revising the ITRs to include Internet Governance issues. Other member states including Iran, Cuba, Kyrgyzstan, Sudan and Bahrain joined Russia and China and formed a coalition to advance this issue. Countries such as the United States, United Kingdom, Italy, Switzerland, Canada, Poland, the Netherlands, and Sweden objected, and emphasized that the WCIT-12 as an intergovernmental forum would not be an appropriate venue for discussing and making decisions about Internet Governance issues. There was failure to reach a consensus about the revision of ITRs at the conference as a result of the profound division between these two blocs. It should be noted that ITU procedure dictates that treaties must be approved by consensus rather than majority vote. For ITU treaties to be adopted and become binding international law, Member States must negotiate until a final consensus agreement is reached. Given the impasse between the two rival blocs, the conference chair took the unprecedented step of acting against ITU procedure and finalized the revised text of ITRs based on majority vote rather than consensus. The final text, which included a resolution entitled "To foster an enabling environment for the greater growth of the Internet", was in line with the Russian-led bloc and against those countries

---

411 ITU. "Transcript of the Plenary 3, WCIT-12." *The International Telecommunication Union (ITU)*. 04 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec4plenary3.docx>.

who wanted Internet related issues to stay outside of ITU authority.[412] At the end of the conference the 55 Member States who opposed to the Russian-led bloc refused to sign the final treaty, while 89 Member States supporting the Russian proposal signed it (Figure 5.2). The absence of consensus among all member states prevented the revised ITRs from becoming International law, a grave failure for the ITU given that this had been the main objective of WCIT-12 in the first place. At the same time the WCIT-12 experience can be viewed as a success for countries like Iran who managed to gain support from a majority of countries for their Internet Governance agenda in which governments and intergovernmental institutions such as ITU would play dominant roles.

Figure 5.2: Country Positions on the WCIT-12 Final Acts [413]



[412] ITU. "Final Acts of the World Conference on International Telecommunications (WCIT-12)." *The International Telecommunication Union (ITU)*. 2012. Web. 10 Dec. 2016. <https://www.itu.int/pub/S-CONF-WCIT-2012/en>.

[413] "Signatories of the Final Acts: 89." World Conference on International Telecommunications (WCIT-12). *The International Telecommunication Union (ITU)*, 14 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/osg/wcit-12/highlights/signatories.html>.

5.4. The 2013 World Telecommunication/Information and Communication Technology Policy Forum (WTPF)

The Ahmadinejad administration continued promoting its sovereigntist and government-centric agenda for the duration of its term in office. The final major event on global Internet Governance at which it would do so was the Fifth World Telecommunication/Information and Communication Technology Policy Forum (WTPF), held by the ITU in Geneva on 14-16 May 2013. Unlike the WCIT-12, participation in the WTPF was not restricted to ITU Member States and its outcome was non-binding. The forum was simply a place where government and non-government members had an opportunity to discuss key policy issues about ICTs including Internet Governance. The main contribution of the Iranian delegate to the forum was the comments it made on the ITU Secretary General's Report to the forum. As the main working document of the forum, this report incorporated the contributions of participants to reach conclusions on key ICT related policy issues. In its comments on the report the IRI criticized the decentralized and bottom-up Internet Governance regime, questioning why the report would not give a more leading role and authority to governments instead of frequently emphasizing the multi-stakeholder framework of Internet Governance. The report had also highlighted the value cyberspace could have as a platform for democratic expression and representation of many cultures, languages, and communities across the globe. The IRI, however, was quick to ask for the exclusion of the potential of cyberspace for democratic expression, instead highlighting the negative aspects of freedom of expression, presumably to justify the comprehensive regime of Internet censorship in Iran that had arisen to an unprecedented level under Ahmadinejad presidency:

> Internet has been used as a tool/means to disseminate false, untrue, misleading, inciting, provocative information, propaganda, cultural attack which have had adverse impact on culture, dignity, customs, tradition, conviction belief, friendship, family life, honor of peoples in certain circumstances, and for certain countries as well as social instability, security, integrity, unity, solidarity, integrity, political stability and peace in certain other countries.[414]

The IRI further proposed that freedom of expression and access to information in cyberspace should be based on "the observance of national legislation, cultural heritage, historical traditions and customs and conviction and belief of peoples in individual countries", with governments as the only authority to define the above terms.[415]

Although concerns about western cultural hegemony had been raised by the IRI in past Internet Governance forums, its position on the use of the Internet for what it viewed as "cultural attacks" was an indication that, in the years leading up to the Fifth WTPF, this concern had intensified. Since the 2009 Green Movement, the IRI had come to view cultural attacks, or in its most extreme form called as "soft war", as a premier national security threat. Soft war is defined by the IRI's leadership as an effort by its rivals, particularly the West, to disseminate their cultural and political values and ideals to attract Iranians to themselves and away from the Islamic Republic. In the long-term, this can result in the loss of influence of the regime's own cultural and political ideals over Iranians. The Internet is seen by the IRI leadership as one of the most powerful conduits of soft war. As discussed at length in chapter two, no less than Iran's Supreme Leader Ayatollah Ali Khamenei has been at the forefront in formulating the soft war discourse.

---

414 ITU. "Comment From the Administration of the Islamic Republic of Iran on Fourth Draft of the Secretary-general's Report For the Fifth World Telecommunication/information and Communication Technology Policy Forum 2013." *The International Telecommunication Union (ITU)*. 2013. Web. 10 Dec. 2016. <www.itu.int/md/dologin_md.asp?id=S13-WTPF13IEG3-C-0005!!MSW-E>.

415 Ibid.

He compares this struggle to the threats posed by the Western powers to the IRI during its traumatic first decade of revolution and war (1979-1989). According to Ayatollah Khamenei, while the IRI had initially been confronted with *hard* military and economic threats by these rivals, their priority in more recent years had shifted to *soft* cultural and political threats using novel information and communication technologies.[416]

The main response of the Iranian government to what it perceives as an increasingly serious threat has been a comprehensive filtering regime to limit generation and distribution of and access to content that rivals the political and cultural ideals and values of the Islamic Republic. As Falasiri and Ghanavizi have noted, under Ahmadinejad "approximately five million websites, social networks such as Facebook, and blogs were filtered, and many dissident bloggers were imprisoned".[417] By the end of Ahmadinejad's tenure, such measures had ensured that there was an unprecedented level of restrictions over Iranian cyberspace. In this context, the IRI delegation's above remarks at the Fifth WTPF can be seen as an attempt to promote a global Internet Governance regime that recognised as legitimate, or at least did not actively confront, restrictive Iranian measures in cyberspace.

As mentioned previously, advocates of multi-stakeholderism in Internet Governance argue that the ITU is an intergovernmental body and, in the absence of NGOs, is not an appropriate venue for discussion of Internet Governance. To address this concern the ITU Secretary General's

---

[416] Khamenei, Ali. "Bayanat Dar Jam-e Kasiri Az Basijian-e Keshvar (A Speech to a Large Crowd of the Nation's Basij)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei*. 25 Nov. 2009. Web. 26 Oct. 2017. <http://farsi.khamenei.ir/speech-content?id=8430>.

[417] Falasiri, Arash, and Nazanin Ghanavizi. "The Persian Blogosphere in Dissent." *Social Media in Iran: Politics and Society after 2009*, Ed. David M. Faris and Babak Rahimi. Albany: State University of New York Press, 2015. 123-36. p.132.

Report emphasized NGOs would be entitled and encouraged to join the ITU as members. In response, the IRI called for the report to underline that participation of NGOs in the ITU had to observe the conditions and criteria mentioned in Article 19 of the ITU Convention and Resolution 145 (Antalya 2006).[418] A close reading of the Convention and Resolution show that non-state entities and organizations willing to become Sector Members with the right to vote in the ITU venues need to first be approved by the concerned Member State. The IRI emphasis on these provisions and criteria of participation of NGOs in the ITU was clearly indicative of the IRI's desired Internet Governance agenda in which the governments would have ultimate authority. It was also indicative of the ITU's fundamental shortcomings when it came to embracing a multi-stakeholder Internet Governance framework in any meaningful way. In the absence of substantive reform in the ITU to guarantee the representation of genuine and independent NGOs in Internet Governance decision making processes, simply just recognizing multi-stakeholderism in the organization's documents will be viewed by many as little more than window dressing over a larger problem. As such, the ITU as an inter-governmental body will remain an inappropriate venue for making decisions about Internet Governance. These shortcomings paved the way for multi-stakeholder global forums to once again take a leading role in Internet Governance. Chief among them was NETmundial.

---

[418] ITU. "Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference (Edition 2015)." *The International Telecommunication Union (ITU)*. 2015. Web. 10 Dec. 2016. <https://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000155201PDFE.PDF>.

5.5. Netmundial: The Global Multistakeholder Meeting on the Future of Internet Governance

In August 2013, the Mahmoud Ahmadinejad presidency came to an end with the elevation of Hassan Rouhani as president. On several occasions during his campaign, Rouhani criticized the restrictive policies of the Ahmadinejad administration towards the Internet. In July 2013, for instance, then presidential candidate Rouhani harshly criticized the proponents of these restrictive policies:

> They are afraid of the freedom which exists in this space, they seek to limit the news, and these limitations will not be successful. I wish the supporters of filtering would explain which news they have succeeded in limiting the people's access to? Which important news in the last few years could filtering prevent people from accessing? These actions have not even become an obstacle to accessing immoral websites. Mass filtering had no other benefits except in thickening the walls of distrust between the people and government, harming our economy, and being an obstacle to the development of the positive uses of the Internet in Iran.[419]

After his victory, Rouhani who had taken note of the way in which his supporters utilized cyberspace to break the media monopoly of Iranian hardliners and mobilize people behind his campaign, became even more determined to reverse the restrictive cyber policies of his predecessor. This shift in Iranian domestic politics toward cyberspace was reflected in the agenda presented by the IRI at the global Internet Governance venues under the Rouhani presidency.

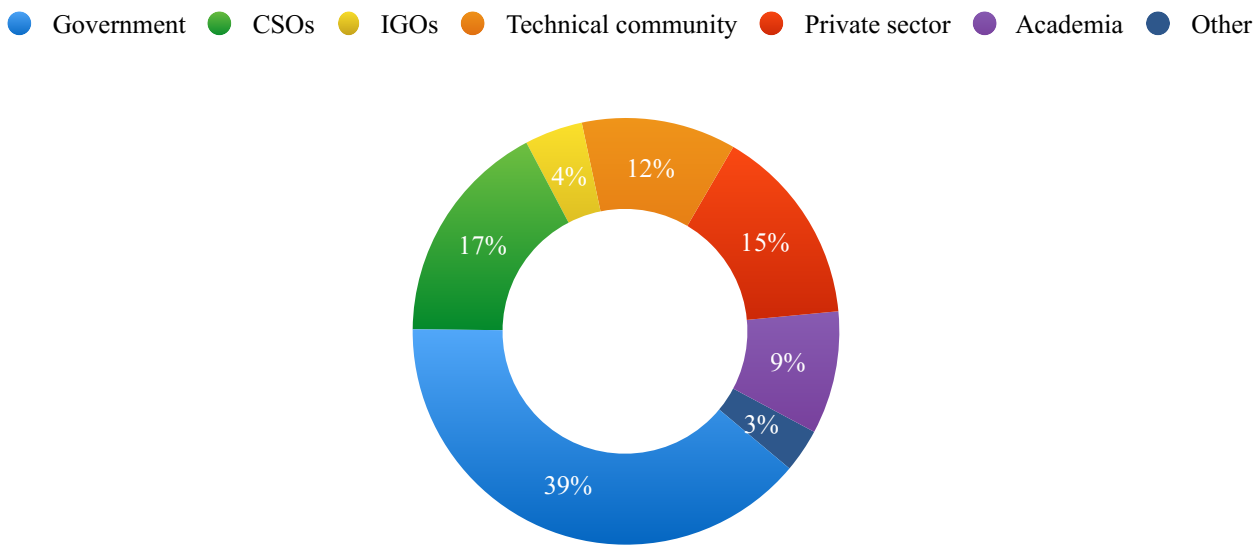
The first global Internet Governance event the IRI attended under the Rouhani presidency was the Global Multistakeholder Meeting for the Future of the Internet, also known as NETmundial, hosted

---

[419] Rouhani, Hassan. "Didgah-haye Raees-e Jomhur-e Montakhab Darbareh-ye Filtering, Faza-ye Majazi Va Donyaye Ertebatat (The President-elect's Viewpoints about Filtering, Cyberspace and Communication World)." *Information Technology News Agency (ITNA)*. 01 July 2013. Web. 10 Dec. 2016. <http://itna.ir/fa/doc/interview/26665>.

by the government of Brazil. NETmundial was held on 23-24 April 2014, in Sao Paulo, where more than 900 participants from a wide range of sectors, including government, private sector, civil society, academia, and the technical community, came together to discuss Internet Governance issues in the largest international meeting since the failed WCIT-12.[420] (Figure 5.3)

Figure 5.3: Percentage of Participating Stakeholders in NETmundial by Type



An analysis of the IRI's contribution to the meeting shows how Rouhani's agenda was, to a large degree, a return to Khatami's Internet Governance agenda presented in the first phase of the WSIS in Geneva in 2003. Unlike the IRI's agenda under Ahmadinejad which had undermined protection of human rights in cyberspace and at one point even called for the exclusion of the democratic expression from the outcome document of a global Internet Governance venue, the Rouhani agenda at NETmundial emphasized that "Freedom, privacy and human rights must be considered and recognized" as a fundamental principle of the regime of Internet Governance in

[420] Almeida, Virgilio A.f. "The Evolution of Internet Governance: Lessons Learned from NETmundial." *IEEE Internet Computing* 18.5 (2014): 65-69.

the meeting's outcome.[421] On the issue of multi-stakeholderism versus government-centrism too the agenda took a different direction from the previous administration and called for a global regime of Internet Governance based on a multi-stakeholder model, highlighting that: "International nature of the governance in which all stakeholder participate, according to their role and responsibilities must be recognized so as no single government (s) retains any legacy or dominate that governance."[422] Regarding the role of ICANN in global Internet Governance, the IRI's agenda had two main pillars: First, like the Khatami agenda, it emphasized that the meeting must move towards undoing US influence and control over ICANN and the domain name system. Second, it called for ICANN to be restructured or replaced by a new organization based on the multi-stakeholder framework of Internet Governance. This approach was different from countries such as China and Russia, which utilized the US influence and control over ICANN as a pretext to advocate replacing it with a new intergovernmental organization. While opposing the US oversight of ICANN, the IRI agenda supported the idea of multi-stakeholderim over government-centrism regarding Internet Governance. Moreover, while the IRI was not necessarily opposed to the idea of replacing ICANN, it did not insist on it and was in fact open to the idea of reforming the organization to be more transparent and inclusive. This approach garnered support from the majority of participants and was ultimately enshrined in the meeting's non-binding resolution called "NETmundial Multistakeholder Statement". The resolution called for an open consensus driven regime of Internet Governance with the participation of all stakeholders: "Internet Governance should be built on democratic, multi-stakeholder processes,

---

[421] NM. "Contribution from the Islamic Republic of Iran to The Global Multistakeholder Meeting for the Future of the Internet, 23-24 April 2014 Sao Paolo, Brazil." *NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance*. 2014. Web. 10 Dec. 2016. <http://content.netmundial.br/files/236.pdf>.

[422] Ibid.

ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users."[423] The resolution also called for the transition of ICANN to a global multi-stakeholder organization, emphasizing that: "This transition should be conducted thoughtfully with a focus on maintaining the security and stability of the Internet, empowering the principle of equal participation among all stakeholder groups and striving towards a completed transition by September 2015."[424] The resolution was approved by an absolute majority of the participants. NETmundial demonstrated that the extent to which, since the failure of WCIT-12 and in contrast to it, governments had become more open to multi-stakeholder framework of Internet Governance as shown by the majority acceptance of the final statement of the event. It also showed how a meeting in which all of the relevant stakeholders participated and exchanged views could allow for the emergence of consensus, even on highly divisive issues on the future of global Internet Governance.

Although there has been a noticeable shift in policies toward global Internet governance under Rouhani when compared to Ahmadinejad, this shift has been less pronounced than Rouhani's rhetoric would suggest. Is this simply the case of a politician reneging or scaling back on promises once in power? Evidence suggests that a more structural explanation involving recent changes to how cyber policy is formulated in the Islamic Republic may be in order. As discussed in detail in chapter three, Iranian Supreme Leader Ayatollah Ali Khamenei ordered the creation

---

[423] NM. "NETmundial Multistakeholder Statement." *NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance*., 24 Apr. 2014. Web. 10 Dec. 2016. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

[424] Ibid.

of the Supreme Council for Cyberspace (SCC) in March 2012. The SCC is tasked with the comprehensive supervision of cyberspace on the domestic and international levels, decision-making on governing this domain, and overseeing implementation of the decisions it makes. Furthermore, the council is by law the highest governing body dealing with cyber issues, with authority in this area that exceeds the executive, legislature, and judiciary, meaning the branches of government cannot challenge the council's decisions on cyberspace. An analysis of the membership of the SCC can give insight on where control over the cyber policy making process truly lays in the Islamic Republic since the formation of the SCC in 2012. Although headed by the president, a majority of the SCC members are appointed by the supreme leader. This means that the majority of the membership of the SCC, in one way or another, represent the supreme leader, thereby giving him profound sway in the direction of cyber policy and limiting the role that the president plays. This shift has already begun to have reverberations on a wide range of issues, including how the IRI approaches global Internet Governance. At the 2013 NetMundial meeting, for instance, Iran's contribution was a product of the Cyberspace National Council (CNC), a body which is subordinate to the Supreme Cyberspace Council. Since the role of the executive branch in cyber decision-making has been diminished, we can expect to see fewer fluctuations in the IRI's positions on global Internet Governance resulting from the regular election and departure of presidents. Instead, the IRI is likely to have a more consistent agenda that favours greater restrictiveness in cyberspace and more sovereigntist and government-centric positions on global Internet Governance, in large part due to the domination of the SCC by principlists.

5.6. WSIS+10: The United Nations General Assembly High-level Meeting of Internet Governance

The last major global Internet Governance event during the presidency of Hassan Rouhani was the WSIS+10 General Assembly High-level Meeting in 2015 to review the overall of progress made in the implementation of WSIS outcomes. This event had its genesis in paragraph 111 of the Tunis Agenda, the main outcome document of the second phase of WSIS in 2005, which requested the United Nations General Assembly (UNGA) to review the implementation of WSIS outcomes in 10 years. Accordingly, UNGA resolution 68/302, adopted on 31 July 2014, decided that the overall review would be concluded in a two-day UNGA high-level meeting.[425] During the second preparatory meeting prior to WSIS+10, the IRI delegation emphasized the integral role of ICTs in inclusive social and economic development, calling on the United Nations to promote the utilization of ICTs as a catalyst to fulfill the Sustainable Development Goals (SDGs). These goals, enshrined in United Nations Resolution A/RES/70/1 which was entitled "Transforming Our World: The 2030 Agenda for Sustainable Development," are a set of seventeen objectives covering a broad range of sustainable development issues (Table 5.2).[426] Coming as a successor to the eight Millennium Development Goals that had been set for the year 2015, the SDGs are the main agenda for development until the year 2030. The critical link between the utilization of ICTs for the achievement of SDGs were also emphasized by many other Global South countries in their contributions to the WSIS+10 preparatory process.

---

[425] UN. "68/302. Modalities for the Overall Review by the General Assembly of the Implementation of the Outcomes of the World Summit on the Information Society." *The United Nations*. 13 Aug. 2014. Web. 10 Dec. 2016. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/302>.

[426] UN. "70/1. Transforming Our World: The 2030 Agenda for Sustainable Development." *The United Nations*. 21 Oct. 2015. Web. 10 Dec. 2016. <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E>.

Table 5.2: The United Nations Sustainable Development Goals (SDGs)

1. NO POVERTY	2. ZERO HUNGER	3. GOOD HEALTH AND WELL-BEING	4. QUALITY EDUCATION	5. GENDER EQUALITY	6. CLEAN WATER AND SANITATION
7. AFFORDABLE AND CLEAN ENERGY	8. DECENT WORK AND ECONOMIC GROWTH	9. INDUSTRY, INNOVATION AND INFRASTRUCTURE	10. REDUCED INEQUALITIES	11. SUSTAINABLE CITIES AND COMMUNITIES	12. RESPONSIBLE CONSUMPTION AND PRODUCTION
13. CLIMATE ACTION	14. LIFE BELOW WATER	15. LIFE ON LAND	16. PEACE, JUSTICE AND STRONG INSTITUTIONS	17. PARTNERSHIP FOR THE GOALS	

The groundswell of support for this concept meant that it was incorporated into paragraph 12 of UNGA resolution 70/125, the main WSIS+10 outcome document, which read:

> We commit to harnessing the potential of information and communications technologies to achieve the 2030 Agenda for Sustainable Development and other internationally agreed development goals, noting that they can accelerate progress across all 17 Sustainable Development Goals. We accordingly call upon all Governments, the private sector, civil society, international organizations, the technical and academic communities and all other relevant stakeholders to integrate information and communications technologies into their approaches to implementing the Goals, and request United Nations entities facilitating the World Summit on the Information Society action lines to review their reporting and work plans to support implementation of the 2030 Agenda.[427]

On the issue of critical Internet resources management, the IRI delegation advocated the establishment of a multilateral, democratic, and transparent model of Internet Governance. At the same time, the Iranian delegation emphasized their country's long standing opposition to

[427] UN. "70/125. Outcome Document of the High-level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society." *The United Nations*. 1 Feb. 2016. Web. 10 Dec. 2016. <http://unctad.org/en/PublicationsLibrary/ares70d125_en.pdf>.

unilateralism by any state, a tacit reference to the United States, calling for all governments to have an equal say in the international public policy issues related to the Internet. The IRI agenda also raised concerns regarding cyber-attacks, a unique aspect which had never been explicitly included in IRI deliberations in various global Internet Governance forums since 2003. As one the first victims of offensive cyber operations in the form of the Stuxnet worm in 2010, the IRI underlined that "the absence of international regulations on cyber-security including cyber-attacks causes adverse effects to ensure the use of ICTs for development. In this regards, we call for the consideration of specific, effective and urgent international measures to counteract and tackle illegal use of cyberspace to harm other countries."[428] The Iranian position should be understood in the context of attempts made by the United Nations to reconcile international law with cyberwarfare. In their 2013 report the United Nations Group of Governmental Experts (UN GGE) agreed in principle that the bodies of international law most relevant to armed conflicts, including the UN Charter and the Law of Armed Conflict (LOAC), are applicable and in fact essential to maintaining peace, security, and stability of cyberspace.[429] These laws include, among others, the requirement that a state engaging in armed conflict use force as a last resort; distinguish between military and civilian targets; and observe the principle of proportionality which requires that the expected collateral damage be minimized and not excessive in relation to the expected military benefit. The application of international law to cyber warfare pursued by

---

[428] UNPAN. "Statement by Delegation of the Islamic Republic of Iran 2nd Second Preparatory Meeting for the General Assembly's Overall Review of the Implementation of the Outcomes of the WSIS." *United Nations Public Administration Network*. The United Nations, 22 Oct. 2015. Web. 10 Dec. 2016. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN95484.pdf>.

[429] UNIDR. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Institute for Disarmament Research*. The United Nations, 24 June 2013. Web. 10 Dec. 2016. <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf>.

the United Nations was in line with the recommendations that the IRI made on the draft of the UN GGE report:

> As a general principle, international law is applicable and therefore should be applied to the use of information and telecommunications technologies and means by States. For that reason, in their use of these technologies and means, States must observe the purposes and principles of the United Nations and their obligations under its Charter, in particular Article 2, paragraph 3, to settle international disputes by peaceful means, the prohibition in Article 2, paragraph 4, on the threat or use of force in any manner inconsistent with the purposes of the United Nations, as well as the prohibition set out in Article 2, paragraph 7, on intervention and interference in the internal affairs of States.[430]

Parallel to the UN attempt to reconcile international law with cyber warfare and during the same time in 2013, a group of NATO legal scholars formulated the application of the principles of proportionality, discrimination and collateral damage of armed conflicts in cyberspace in the Tallinn Manual on International Law Applicable to Cyber Warfare.[431]

Conclusion

The desire to exert control by state and non-state actors over cyberspace combined with the inherently global architecture of this space have given rise to global institutions of Internet Governance. The decision-making and agenda setting embedded in these institutions in turn constitute one of the main aspects of exercise of power in cyberspace. This chapter analyzed the Internet Governance agenda presented by the IRI in global events since 2003 and illustrated that this agenda has been mainly preoccupied with three major issues.

---

[430] UN. "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General." *The United Nations*. 09 Sept. 2013. Web. 10 Dec. 2016. < http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156/Add.1>.

[431] Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013.

The first issue is the digital divide. In nearly all Internet Governance forums since 2003, the IRI has emphasized that bridging the digital divide is the main requirement for realizing the huge potential of the Internet for economic development. It must be noted that the IRI emphasis on bridging the digital divide has been unevenly focused on the inequalities between states and, as a result, has in fact obscured the inequalities within nations. This is specifically the case in the IRI agenda under Ahmadinejad, which indicated that his administration prioritized the balance of economic power between states over empowering society, with the latter being relegated to an issue of secondary importance. The emphasis on the digital divide and the significance of the Internet in economic development, however, is not unique to the IRI and can be found across the developing world. For this reason, it has been reflected in nearly all outcome documents of global Internet Governance forums and become a main pillar of the emerging global regime of Internet Governance.

The second issue is the dominant role of Global North countries, particularly the United States, in controlling the critical Internet resources through organizations such as ICANN. The IRI challenged this domination and called for all states to have an equal say in the management of the critical Internet resources. Although the principlist presidency of Mahmoud Ahmadinejad seemed to be more vocal in this regard, this was also pursued quite actively by the Mohammad Khatami and Hassan Rouhani administrations. This consensus is not limited to Iranian governments of different political stripes: A majority of states used different global Internet Governance forums to support this idea and, as a result, in March 2014 the United States announced that it would relax its supervision of ICANN and turn it over to a global multi-stakeholder community.[432]

---

[432] NITA. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." *National Telecommunications and Information Administration.* United States Department of Commerce, 14 Mar. 2014. Web. 10 Dec. 2016. <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

The third major issue is the role of non-state actors, such as the private sector and CSOs, in Internet Governance. Contrary to the first and second issues, this one has revealed division between different Iranian administrations. Ahmadinejad's government-centric agenda for Internet Governance sought to severely limit the role of NGOs in order to enhance the hegemony of the state vis-à-vis Iranian society. Khatami and Rouhani, however, acknowledged the role of NGOs and were more open to the multi-stakeholder framework of Internet Governance. This difference should be mainly understood in the context of the diverging agendas of these administrations in terms of the relationships between the government, private sector, and CSOs at the domestic level. The Ahmadinejad administration sought to mobilize the nation's resources for economic development through state-led initiatives and actively suppress CSOs seeking political and social reforms. The Khatami and Rouhani administrations, in contrast, advocated a greater role for the private sector in economic development and sought to empower CSOs in order to advance their political and social reforms.

It appears that the Ahmadinejad model for dealing with the role of non-state actors in Internet Governance at home and abroad is unlikely to succeed in the long-term since non-state actors are key players in cyberspace. Much of the critical Internet resources and infrastructure is owned and managed by the private sector, meaning they are essential mediaries for states to take action in the cyber domain. Take for instance the desire by a state to conduct police action in cyberspace, such as taking down websites dealing with illicit activities like terrorism, hate crimes, and distribution of child pornography. Not only does a state need to call upon a private sector actor, which may very well not be in its jurisdiction, to shut down such a website, but will also have to rely on them to acquire the financial intelligence necessary to track down and prosecute the

criminals behind such illegal activities. This position within cyberspace has allowed the private sector to gain a voice in global forums, advance a multi-stakeholder agenda, and influence outcome documents of these forums such that they have carved out a place for themselves.

Civil society organizations have also been able to find a place for themselves in global Internet Governance through the multi-stakeholder model, albeit in a manner distinct from the private sector. Among other thing, CSOs have been active in promoting the protection of human rights in cyberspace. As a result of a joint effort by Brazil, Nigeria, Sweden, Tunisia, Turkey, and the United States, and with the support of more than 80 CSOs, in June 2016 the United Nations Human Rights Council passed resolution A/HRC/32/L.20 on the "Promotion, protection and enjoyment of human rights on the Internet". The resolution affirms that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."[433] The resolution also calls on all states to ensure accountability in all human rights violations and abuses committed against persons for exercising their human rights and fundamental freedoms on the Internet.

One key issue that has been left off the IRI's agenda of global Internet Governance is the increasingly pervasive phenomenon of transnational cybercrime. The international legal convention to deal with this issue first and most thoroughly is the Budapest Convention on Cybercrime, which establishes a body of cybercrime law and an effective regime of cooperation

[433] UN. "32/13. The Promotion, Protection and Enjoyment of Human Rights on the Internet." *The United Nations*. 18 July 2014. Web. 10 Dec. 2016. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf>.

to implement it, alongside an additional protocol in 2006 dealing with the distribution of racist and xenophobic material. Although this convention took shape in the context of the Committee of Ministers of the Council of Europe, it has not remained an exclusively European regime and has seen countries from around the world join (Table 5.3).[434]

Table 5.3: Signatories of the Budapest Convention on Cybercrime

European Members	Non-European Members
Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The former Yugoslav Republic of Macedonia, Turkey, Ukraine United Kingdom	Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Senegal, South Africa, Sri Lanka, United States of America

Despite having a well developed domestic regime of cybercrime law dealt with in chapter three, the IRI has yet to sign or ratify the Budapest Convention or any similar treaties, leaving a gap in its laws for dealing with transnational cybercrime. This appears to be because Iran has yet to deal with the kind of transnational cyber-criminal activity on a large scale which has become prevalent in many Global North countries in recent years. Such activity includes compromising the confidentiality, integrity and availability of computer data and systems, utilizing cyberspace for forgery and fraud, offenses related to copyright infringement, and the dissemination of racist and xenophobic materials and child pornography. Iran may also be concerned that acceding to

[434] CE. "Chart of Signatures and Ratifications of Treaty 185." *Council of Europe*. 18 Dec. 2016. Web. 18 Dec. 2016. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=X4TZJpSX>.

such a global regime will both create a conflict with its domestic cybercrime law and entail obligations which it is at present unwilling to undertake. However, as Iran's economy is gradually reintegrated into the global economy following the lifting of international sanctions with the implementation of the Joint Comprehensive Plan of Action, and as the Internet becomes more ubiquitous in the country, we may see a rise in transnational cybercrime affecting Iran and therefore an increased willingness on the IRI's part to add this issue to its global Internet Governance agenda.

The multiplicity of actors, wide variety of issues, and the fluidity of shifting priorities over time constitute the complex nature of the emerging global Internet Governance regime. Under the Ahmadinejad administration Iran was not successful in managing this complexity and as a consequence had difficulty contributing to and benefiting from this regime. The Khatami and Rouhani administrations, in contrast, have been more astute in identifying the complex nature of the Internet Governance regime and built the first stepping stones on the path to managing this complexity in a way that enhances Iran's ability to contribute to and benefit from this regime in the future.

CHAPTER SIX: IRAN AND EXERCISE OF CO-OPTIVE POWER IN CYBERSPACE

Introduction

This chapter analyses the last major aspect of power discussed in the theoretical framework chapter: co-optive. Contrary to coercive power which demands obedience and comes from material sources, co-optive power encourages consent and emerges out of ideational sources such as political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. Cyberspace is an important emerging domain for the exercise of co-optive power in which different actors attempt to generate their own sources of co-optive power while countering that of their rivals. States can exercise co-optive power over society by promoting their own political ideals and cultural values in cyberspace, legitimizing their policies in the eyes of citizens. On the other hand, civil society actors can also use the very same domain to promote the political ideals and cultural values at odds with that of the state, countering the state's co-optive power. This is because the main sources from which co-optive power derives are not solely concentrated in the hands of the state, but also reside in civil society actors such as scholars, public intellectuals, social activists and artists, among others.

As discussed in the literature review and theoretical framework, the IRI feels the sense of threat from its domestic and foreign rivals' exercise of co-optive power over Iranian society. The initial response of the IRI to this threat has been to employ coercive measures, explored in chapter three, to block the distribution of rival ideational factors within the country. In more recent years, however, the IRI has found that coercion alone is insufficient to counter the rival ideational factors and, as a result, it has attempted to use cyberspace to deploy its own primary ideational factors to compete with those of its rivals. This chapter attempts to show how different ideational

factors, associated with political ideals, cultural values, policies, and institutions, are generated and debated in Iranian cyberspace.

This chapter has conducted its analysis by focusing on the Instagram social media platform and Telegram messaging application. The rationale behind this selection is that, unlike other social media platforms like Facebook and Twitter, Instagram and Telegram are not banned in Iran, and are also very popular among Iranians, therefore better illustrating trends in Iranian cyberspace. The present study has focused on two broad groups of people in order to analyze the exercise of co-optive power in Iranian cyberspace. These are government officials and public figures, with the latter corresponding to civil society figures with a popular following. As noted above, it is important to look at both groups because the generation of co-optive power and its sources does not exclusively lay in the hands of the state. The time-frame of the present study covers the period between 01 April and 30 June 2017. This period was selected to provide a consistently rich quality and quantity of data in order to conduct this analysis. This is because the selected period not only corresponded to the 2017 Iranian presidential election, during which many important political ideals, cultural values, policies, and institutions were discussed in Iranian cyberspace, but also the tragic attacks of the Islamic State in Iraq and the Levant (ISIL) on Tehran, and the subsequent military response by the Islamic Republic Armed Forces, among other things.

To find the top figures in the generation of ideational factors, measured by their level of activity and influence, the present study found and then surveyed the 10 most followed domestic Iranian media outlets and 10 most followed Persian-language foreign media outlets, with a range of political orientations. These were ranked according to their combined number of Instagram and Telegram followers in figures 6.1 and 6.2.

Figure 6.1: Top Ten Foreign Media Outlets

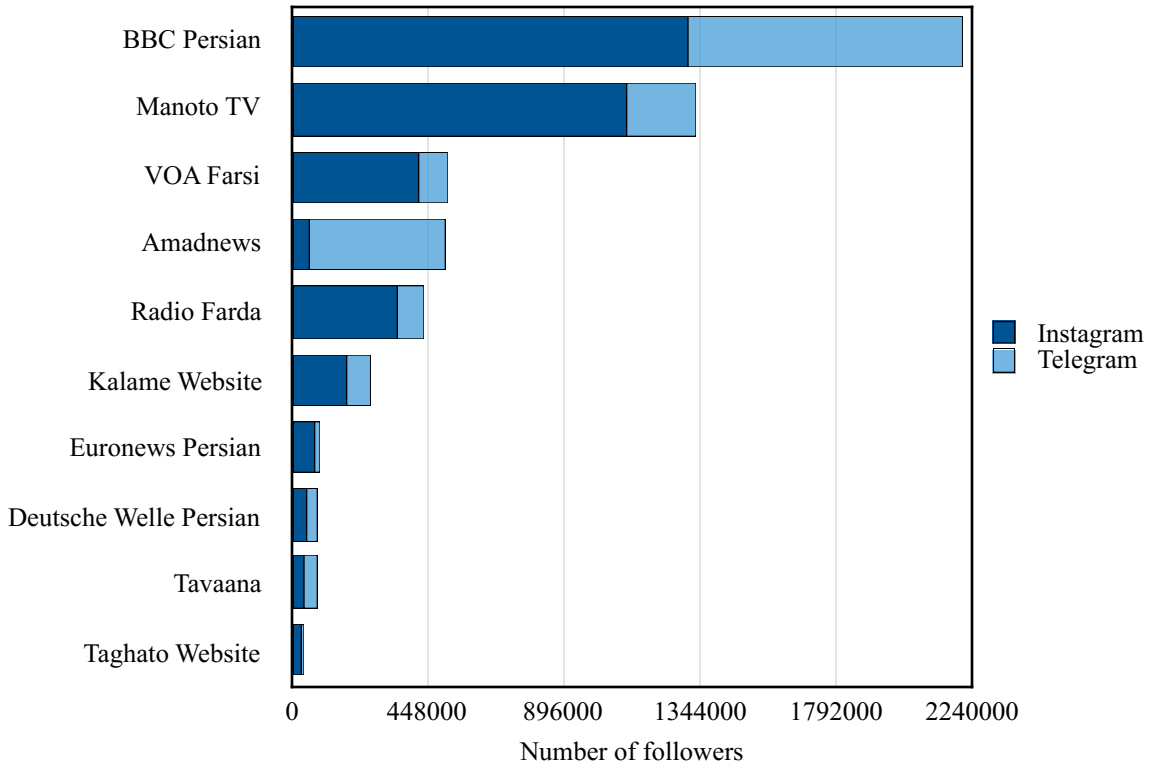
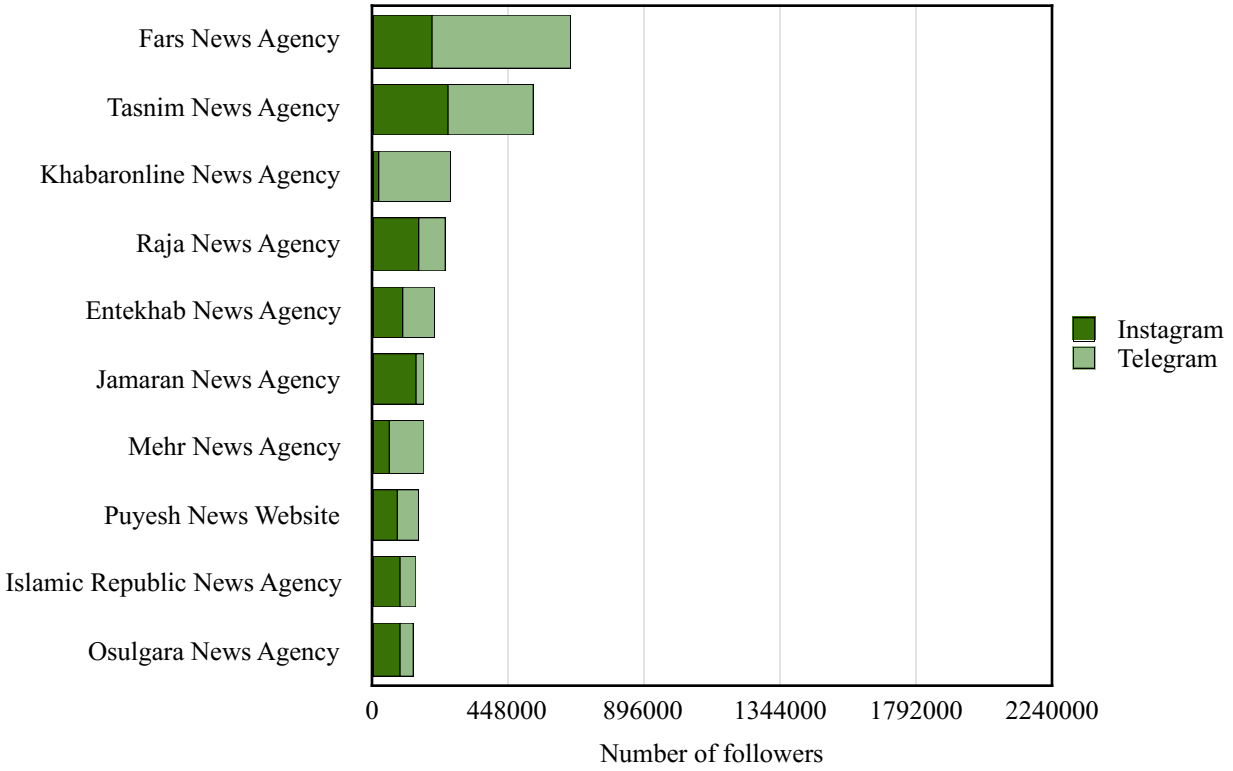


Figure 6.2: Top Ten Domestic Media Outlets



These outlets were surveyed to come up with a list of the top Iranian public figures and government officials whose viewpoints were most widely discussed and circulated in the 20 selected outlets. However, a few side-findings are worth elucidating beforehand here. As figures 6.1 and 6.2 illustrate, the top major foreign news outlets, such as BBC Persian and Manoto, had a larger following than the top domestic news outlets. This mainly corresponds to a higher level of trust in these top foreign outlets versus the top domestic outlets, such as Fars and Tasnim. Conversely, foreign media outlets corresponding to the political opposition against the Islamic Republic, including Simay-e Azadi (Instagram: 438 and Telegram: 3,715), the media arm of the People's Mojahedin Organization of Iran, consistently had the lowest levels of followers and did not make it into the top 10 foreign outlets. A similarly low level of followers could be detected for state media outlets such as Islamic Republic Broadcasting (Instagram: 21,200 and Telegram: 52,023) and Kayhan daily newspaper (Instagram: 33,200 and Telegram: 34,828). IRIB, the well funded main state broadcasting network comparable to the BBC in scale, and Kayhan, among the oldest newspapers in Iran and considered the mouthpiece of Ayatollah Ali Khamenei and the principlist political leadership in Iran, performed poorly despite their various advantages and did not make it into the top 10 domestic outlets.

As already noted, a survey of these media outlets was conducted to come up with a list of the top Iranian public figures and government officials whose viewpoints are most widely discussed and circulated in the selected 20 outlets. From this set, only those with a web-presence on both Instagram and Telegram were selected to establish a greater degree of comparability, and were ranked according to their combined number of followers. This study found that figures from outside of the political establishment of the Islamic Republic did not rise very high, and that the

most highly ranked individuals were consistently figures and officials active within the framework of Islamic Republic. The only exception is Reza Pahlavi (Instagram: 65,500 and Telegram: 44,825), the crown prince of Iran and the leader of the National Council of Iran, an exiled opposition group. Pahlavi has a large following on both Instagram and Telegram platforms, but was not included in the present study because he did not have a presence on Telegram until 11 May 2017, only part way through the period of this study. The main sample of figures used in this study was therefore composed of public figures and government officials who operate within the framework of the Islamic Republic and who had a presence on both Instagram and Telegram. These were in turn divided between the moderate and principlist political camps, the two main political groupings in the Islamic Republic. In total, 20 public figures and 20 government officials were used as the basis for the analysis below, with each set divided evenly between the IRI's two main political groupings (Figures 6.3 to 6.6).

Figure 6.3: Top Ten Moderate Public Figures

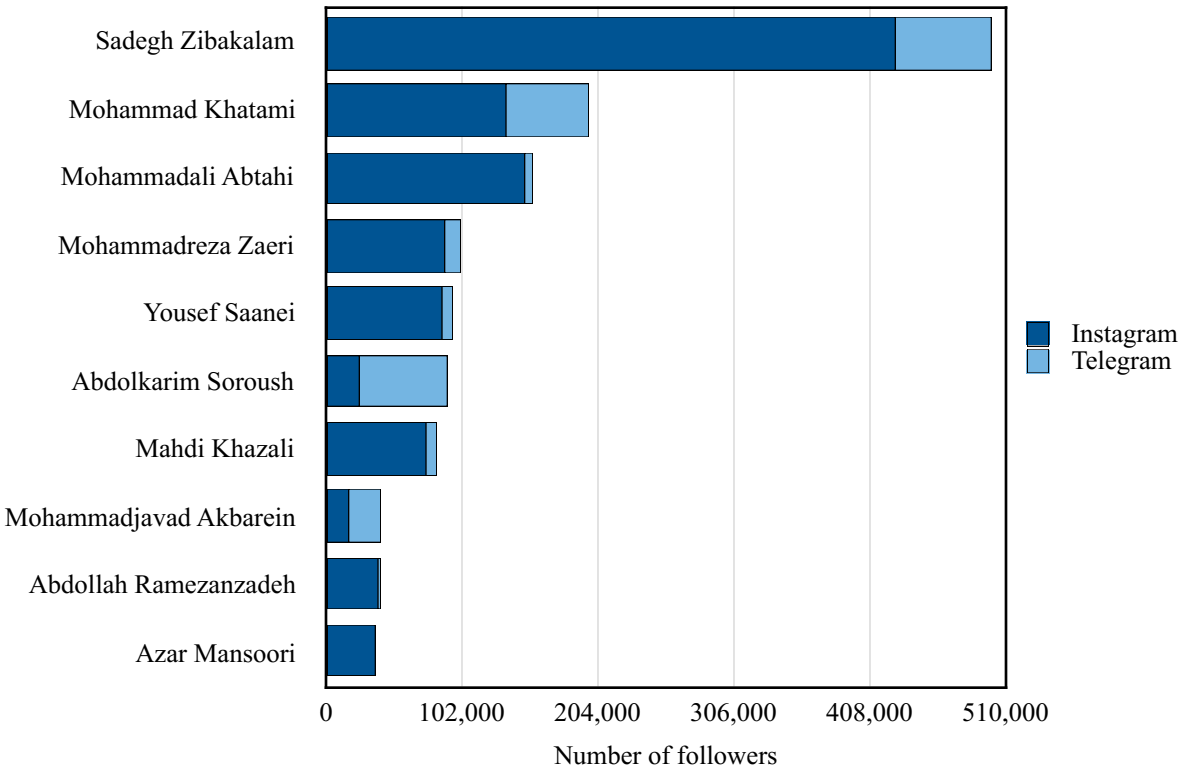


Figure 6.4: Top Ten Principlist Public Figures

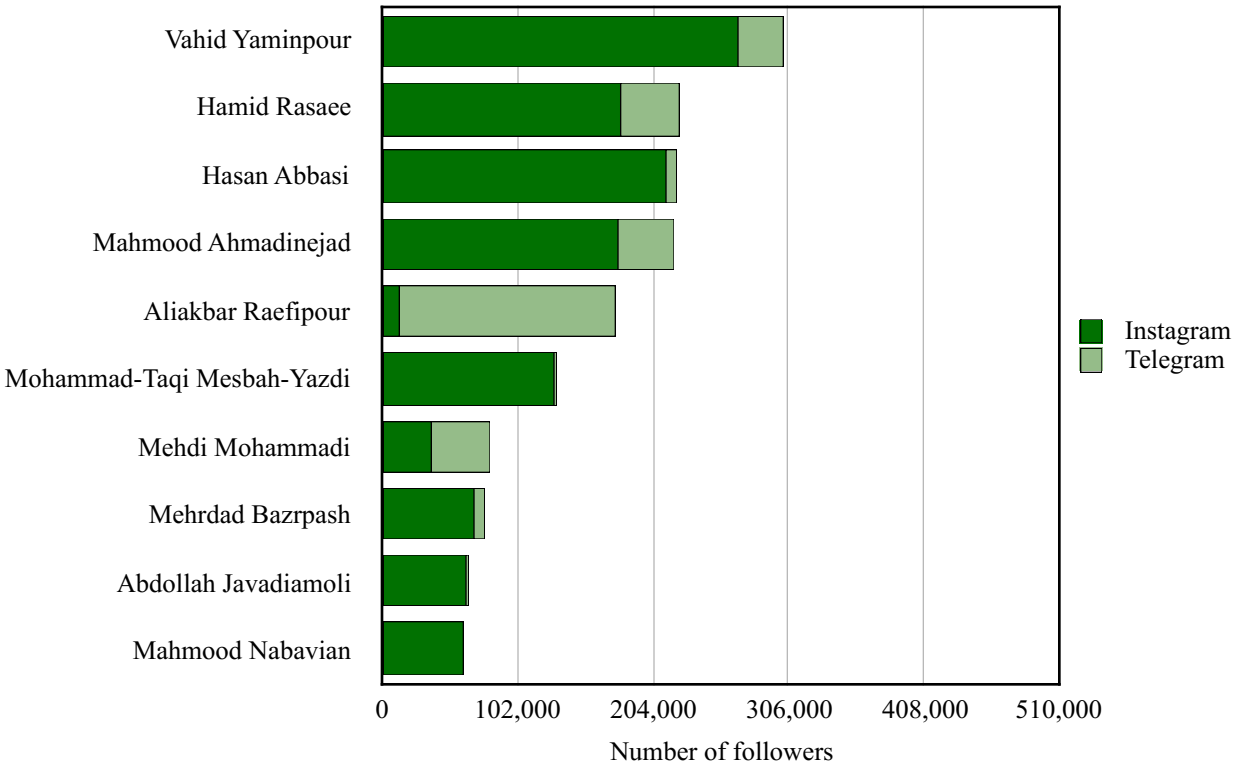


Figure 6.5: Top Ten Moderate Government Officials

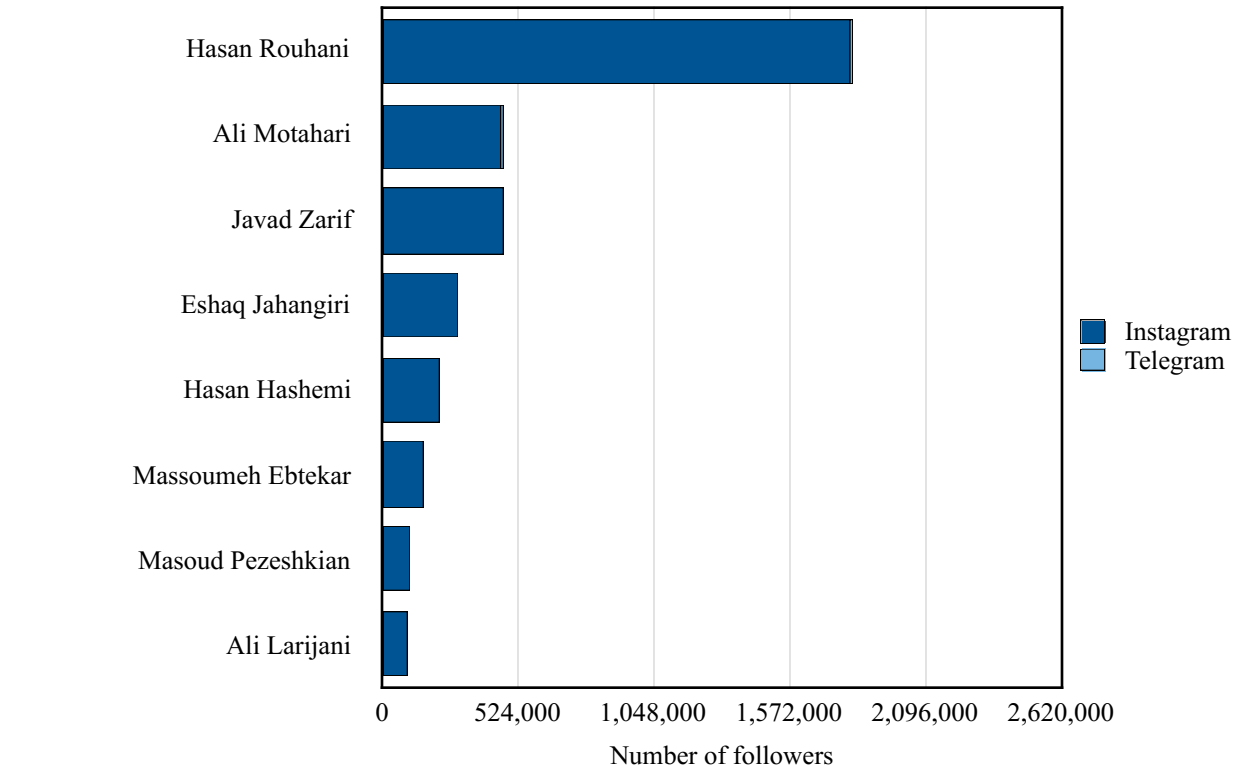
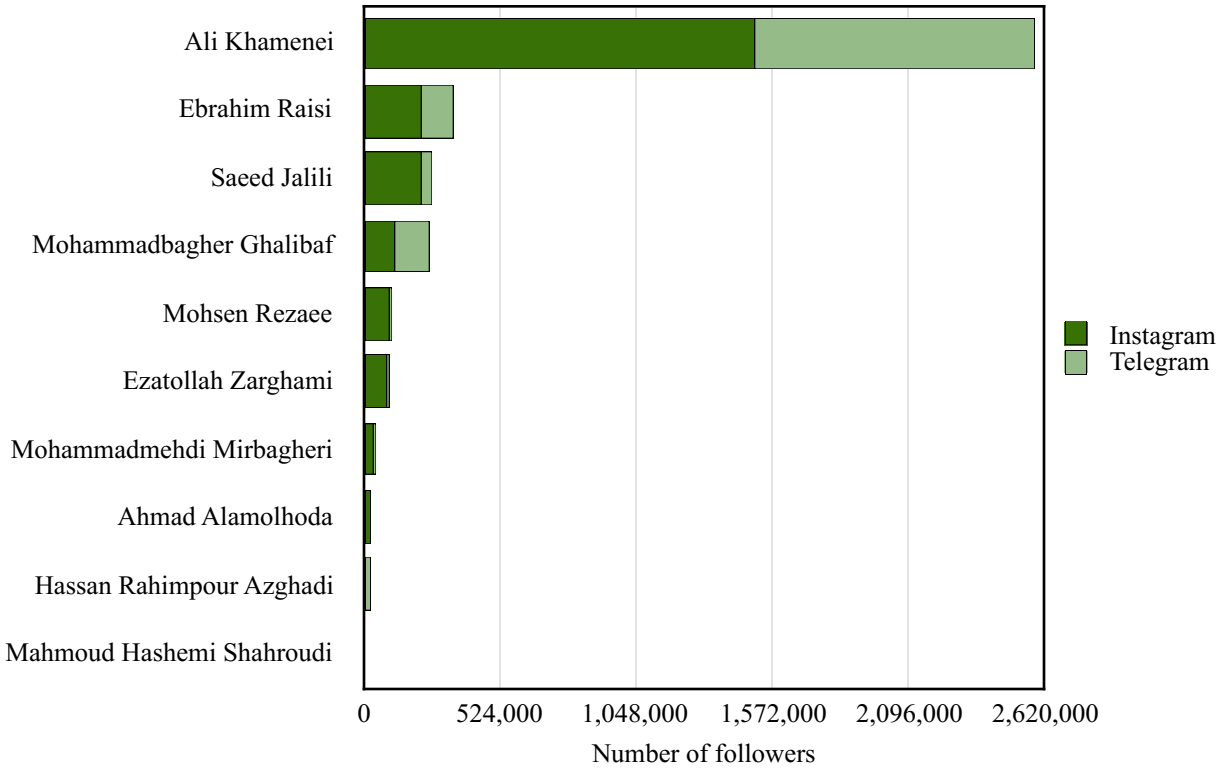


Figure 6.6: Top Ten Principlist Government Officials



As figures 6.3 and 6.4 show, overall, principlist public figures had a stronger web presence than moderate public figures, as measured by the total number of followers on Instagram and Telegram. Moderate public figure Sadegh Zibakalam, however, stands out for having among the highest number of followers of any figure. Conversely, moderate government officials had a stronger web presence than principlist government officials, as measured by the total number of followers on Instagram and Telegram (Figures 6.5 and 6.6). Principlist government official Supreme Leader Ayatollah Ali Khamenei, however, stands out for having among the highest number of followers of any figure. The analysis of the content generated by the moderate camp shows that moderates as a whole focused on the political ideals of socio-political freedoms, whereas principlists emphasized social justice. In the area of policies, moderates advocated

policies that enhanced socio-political freedoms, a more open and private-sector driven economy, and collaboration with other states in foreign policy. Principlists, in stark contrast, advocated policies that limited socio-political freedoms, promoted a more closed, redistributive, and state-driven economy, and a confrontational foreign policy. In terms of the legitimacy and track record of political institutions within the political structure of the Islamic Republic, the analysis shows that moderates and principlists defend elected and unelected institutions, respectively. In order to better frame the qualitative analysis conducted in this chapter, four case studies of public figures and four case studies of government officials, divided evenly between the top-ranked moderates and principlists, have been presented below.

6.1. Public Figures

The following four subsections will present the case studies of the top moderates and principlist public figures who generate ideational factors in Iranian cyberspace.

*6.1.1. Sadegh Zibakala*m

The first case study in this chapter looks at Sadegh Zibakalam, a renowned professor of political science at the University of Tehran. At the level of domestic politics, Zibakalam has been among the major critics of the economic policies of the IRI, especially the Subsidy Plan (*tarh-e yaraneha*). Under President Mahmoud Ahmadinejad, the Iranian government decided to cut subsidies on basic commodities and hand them out in the form of monthly cash disbursements instead. Zibakalam has written a number of posts criticizing the Subsidy Plan with the argument that not only does it not help the poor, but places an undue burden on the state. He noted that in the 1395 Iranian fiscal year (2015-2016), the Iranian government spent 43 trillion toman on

Subsidy Plan cash disbursements that did not narrowly target the poor, but went to all segments of society. He contrasted this to 15 trillion toman Iran had assigned for infrastructure development, meaning cash disbursements cost the government almost three times its entire infrastructure spending during the same fiscal year. He also contrasted this figure to the 5 trillion toman budget assigned for all universities and 300 billion toman assigned to the environment budget, in the context of the ongoing environmental and water crisis in Iran.[435]

In the context of the 2017 Iranian presidential election, Zibakalam tied the Subsidy Plan to the campaign promises made by principlist candidates, including Ebrahim Raisi and Mohammad-Bagher Ghalibaf, to multiply cash disbursements by over five times, as part of their populist platforms to address poverty and unemployment. In a viral post, Zibakalam exclaimed: "Mr. Ghalibaf! Mr. Raisi! Where will you bring the employment budget from? Do you want to cut the military budget? Do you want to cut it from Syria? Do you want to cut it from Lebanon? Do you want to cut it from healthcare? From education?"[436] By raising Iranian spending on the military, Hezbollah in Lebanon, and in support of the war effort by Bashar al-Assad in Syria, issues near and dear to Iranian principlists and candidates like Ghalibaf and Raisi, Zibakalam also broke taboos of criticizing Iranian foreign policy in the Middle East and implicitly raised the question of whether these dollars might not be better spent at home. In another post, he criticized the overall management of the economy in the Islamic Republic, and called for it to "put aside bold but hollow slogans that we have repeated for 30-40 years, such as the model of the Iranian-Islamic economy, the monotheistic economy, the Islamic economy, or the indigenous

---

[435] Zibakalam, Sadegh. *Instagram*, 27 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTaq7l1DIug/>.

[436] Zibakalam, Sadegh. *Telegram*, 09 May 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1556>.

development model and the like". Instead, he said that Iran should go in a direction that has shown its effectiveness in other developing economies around the world.[437]

Zibakalam also criticized the Guardian Council (GC) in his social media posts.[438] A central political institution controlled by principlists, the GC is responsible for determining the qualification of candidates for national elections and therefore acts as a filter against undesired entrants into the system. The GC has not only acted as a filter against political outsiders, but has even served to disqualify current and former stalwarts of the IRI from participating, like former presidents Ayatollah Akbar Hashemi-Rafsanjani and Mahmoud Ahmadinejad. Zibakalam has been consistent in his criticism of the GC, and in the 2017 election spoke out against the disqualification of Ahmadinejad, even though he had been among Ahmadinejad's most vocal critics when he was in office. The Islamic Republic often justifies GC filtering by arguing that every country has a mechanism for filtering candidates. Zibakalam argues that this is a fallacy: "In no regime based on democracy is there a phenomena called determining qualification, because this phenomena is in contradiction with a regime based on the vote of the people. It is only the people themselves who determine who is qualified and who is not qualified." He argues this means that in the Islamic Republic: "Determining qualification has become a political tool in the service of the regime to block the entry of anyone who it finds politically unpalatable."[439]

Zibakalam is known to be equally vociferous in his critiques on social media on Iranian foreign policy. One of his posts addressed the new charter of Palestinian Islamist group Hamas in May of

---

[437] Zibakalam, Sadegh. *Telegram*, 26 June 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1673.

[438] Zibakalam, Sadegh. *Instagram*, 22 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTN0SL7Dq7P/>.

[439] Zibakalam, Sadegh. *Telegram*, 26 June 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1515>.

2017, which accepted the idea of a Palestinian state within the confines of the 1967 borders. Zibakalam argued that the new position showed that, no matter how one interpreted it, Hamas is heading in the direction of refraining from calling for the destruction of Israel. He noted that the Palestinian Liberation Organization had already accepted the existence of Israel in the context of the Oslo Accords, and what the Hamas charter had done was in line with this. Zibakalam explained that the implication of this was that the Islamic Republic was the only country that still called for putting an end to the Zionist regime of Israel. He went on a rhetorical tirade of questions asking who had decided this:

> What authority or institution has given this duty or mission to the IRI? Has the destruction of Israel been articulated in our Constitution? Has it been passed by parliament? Has the United Nations or Security Council given Iran this responsibility? Has the Arab League, Palestinian parliament, Organization of the Islamic Conference, or Non-Aligned Movement asked Iran to destroy Israel? Have the Iranian people voted in a referendum to destroy Israel and, as a result, the Iranian government is responsible for carrying out this demand? Has there even been a simple poll, let alone a referendum, asking the Iranian people's opinion on Israel and its destruction?[440]

He also had another post criticizing Iranian foreign policy after the attack by the ISIL on Tehran in June 2017. Zibakalam targeted what he labelled as Iranian principlists' "political opportunism" in blaming this attack on Rouhani and his foreign policy on the basis that the Iranian president had allowed the attacks to happen by not confronting the West.[441] He pointed out that the basis for this principlist critique of Rouhani, was a conspiracy theory that said ISIL had been created by the West, and Zibakalam created and published six videos on his social media platforms to

---

[440] Zibakalam, Sadegh. *Instagram*, 02 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTmrn9AD090/>.

[441] Zibakalam, Sadegh. *Instagram*, 08 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVEboyQD4jW/>.

discredit this idea.[442] He also noted how the principlists' politicization of the ISIL attack on Tehran had been used to help justify the Islamic Republic's foreign policy in the Middle East and the increasingly prominent role of the Islamic Revolutionary Guard Corps (IRGC) in the country. Zibakalam pointed out if Iran's regional policies and IRGC's role were justified on the basis of stopping terrorism, then they had failed: "Like other ISIL operations, 17 Khordad [attack on Tehran] was a blind act of terrorism. This operation neither proved the correctness of the hardliners' foreign policy nor did it refute Rouhani's moderate foreign policy. It did not justify our policy in Syria and eventually it could not justify the interference of the IRGC in the political and economic affairs of the country."[443]

6.1.2. Mohammad Khatami

Mohammad Khatami, a popular former president of the IRI (1997-2005) and a renowned figure of the reform movement in Iran which advocates for expanded social and political freedoms, is another moderate public figure with a strong presence on social media and a wide appeal. A close analysis of Khatami's cyber-presence shows the way he uses social media to articulate and disseminate his political and philosophical ideas now that he is out of power. One issue Khatami has grappled with has been the problem of underdevelopment in Iran. To address this issue, he has called for a synthesis between a Western development path and the country's indigenous and traditional conditions. However to reach this synthesis, he has criticized both the West and Iranian tradition in order to extract the best of both. For instance, he notes that "I, as an easterner,

---

[442] Zibakalam, Sadegh. *Telegram*, 30 June 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1684.

[443] Zibakalam, Sadegh. *Instagram*, 08 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVEboyQD4jW/>.

when I hear from the West, I remember occupation and imposition of corrupt policies and the despotic rulers dependent on them, and exploitation of resources and suppression. What interpretation do I have as a suppressed easterner, all of whose resources has been exploited."[444] Khatami resolves this by differentiating between the valuable aspects of the West and its negative aspects such as colonialism. The conclusion he draws is that when facing the West, Iranians should not seek to wholly embrace or deny it, but to criticize it. He calls for a similar approach toward the country's traditions. Ultimately, both the West and local tradition have positive and negative aspects, and only a dialectic between the two can produce a positive result, which is wholly divorced neither from the West or local tradition.

A close analysis reveals that by disseminating these ideas among his large social media following, Khatami is engaging in a counter-hegemonic narrative construction to challenge both West-centrist and traditionalists thinkers and ideas, and identify their pathologies. Khatami notes that: "Hatred and infatuation is the great pain of our recent history and the abortive challenge of tradition and modernity that has affected our destiny for 150 years is derived more from these feelings and less a result of thinking."[445] The only environment in which a dialectic between Western modernity and local tradition can take place, that results in a synthesis or model for the way ahead, is a free and democratic society: "In a dictatorial environment minds become distraught and real voices cannot be heard. This is a comprehensive and dangerous malady and

---

[444] Khatami, Mohammad. *Instagram*, 18 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTCDIdNAo1T/>.

[445] Khatami, Mohammad. *Telegram*, 29 May 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/511>.

for its real treatment, freedom and democracy must be defended and the price of their actualization paid."[446]

Khatami also uses his social media following to articulate his worldview on global politics in line with the Dialogue of Civilizations framework he articulated during his presidency. In his social media discourse Khatami criticizes the prevailing structure of international relations on the basis of a number of key arguments. One argument criticizes the realist notion of power which emphasizes military strength: "The military aspect of power is by itself neither effective nor does it create deterrence."[447] This approach, according to Khatami, produces war, a critique which appears to not only be aimed at the superpowers able to project military power, but also implicitly at Iranian principlists, who propagate the same ideals in the domain of foreign policy. Khatami also appears to focus on the theme of what he views as a regressive take on religion which fuels terrorism, epitomized by the Islamic State of Iraq and the Levant (ISIL).[448] An analysis of his social media discourse shows that he returned to this idea following the June 2017 attack by ISIL on Tehran: "The crimes of terrorists are approved by extortionist powers and their allies and sympathizers or at least faced with their indifference…It is not accidental that at the same time as the human-killing terrorists are committing crimes in Iran, in the U.S. Congress there is an effort for the strengthening of sanctions against Iran on the accusation of supporting terrorism."[449] As this quote shows, Khatami links militarism and terrorism as two sides of the

---

[446] Khatami, Mohammad. *Instagram*, 06 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BU_j1ojAdAQ>.

[447] Khatami, Mohammad. *Telegram*, 11 June 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/529>.

[448] Khatami, Mohammad. *Telegram*, 12 June 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/531>.

[449] Khatami, Mohammad. *Instagram*, 10 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVKcVkQgcRC>.

same coin. What is the solution? According to him, a dialogue must take shape that impacts public opinion and creates sensitivity around militarism and terrorism. Such a dialogue must be based on both "reason", which he says manifests itself as science, and "spirituality", which manifests itself as religion. Reason alone cannot address these issues because, as something that can increase destructive capabilities and technology, it actually enhances the capacity for damage. He argues that it must be paired with spiritually: "Our time, in order to gain emancipation, needs religion, a religion that in addition to God believes in justice, freedom, and human right and disbelieves in poverty, ignorance, and war and terror and human degradation."[450]

Perhaps the most important aspect of Khatami's social media discourse has been constant forays into Iranian politics. During the 2016 Iranian parliamentary and Assembly of Experts elections, Khatami used social media, including a now famous video, to mobilize his supporters to strategically vote for all of the candidates on the List of Hope, corresponding with the moderate camp in Iranian politics, in order to prevent principlist candidates from being elected in their locales.[451] This is all the more significant given that Khatami is under a media ban in Iran which prevents him from being shown or even named in the state media. In this instance Khatami's message proved wildly successful and his phrasing in the video, which emphasized the word "repeat" to insist that voters should vote for all of the candidates on the List of Hope, became iconic. His peculiar use of the word "repeat" found its way into print media headlines and social media hashtags and memes. The virality of this message allowed him to repeat this formulation in another video in support of President Hassan Rouhani in the 2017 Iranian presidential

---

[450] Khatami, Mohammad. *Telegram*, 13 June 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/533>.

[451] Khatami, Mohammad. *Telegram*, 21 Feb. 2016. Web. 02 Sept 2017. <https://t.me/khatamimedia/150>.

election, in which he declared: "And this time it is you who must *repeat* it, *repeat* the vote for dear Rouhani, for strengthening hope in a better future."[452] In this video Khatami supported the Rouhani administration and its track record in a number of domains, especially the Joint Comprehensive Plan of Action (JCPOA), or Iran nuclear deal, which he has called a "shining page in the record of the Rouhani administration." He also uses his social media platform to warn Iranians against populist campaign slogans articulated by the principlist candidates: "Never must one be fooled by illusory and baseless slogans for resolving problems. Some of these slogans are not, firstly, practical, second if they are practical they will create serious crises in society that in the first place will blowback on those in poverty."[453] Khatami is not only the creator of such viral messages, but also an object of viral messages by ordinary Iranians, like the hundreds of people who photographed and live-streamed his vote in the 2017 election to break the media ban imposed on him by authorities.[454]

6.1.3. Vahid Yaminpour

The principlist political current in the IRI mirrors the moderate camp in its use of social media. Vahid Yaminpour is just one example of a young, popular, and prominent principlist figure with a large social media reach. Yaminpour has been a host of several television programs on state television and published relatively widely on Islamic culture. Yaminpour has been a critic of the Hassan Rouhani administration on issues of domestic politics and foreign policy, including the

---

[452] Khatami, Mohammad. *Telegram*, 14 May 2016. Web. 02 Sept 2017. <https://t.me/khatamimedia/468> (Emphasis added).

[453] Ibid.

[454] Khatami, Mohammad. *Instagram*, 19 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BURNx7ZAoZh/>.

JCPOA. On the anniversary in 2017 of the failed US Operation Eagle Claw to rescue American hostages in Iran in April 1980, Yaminpour proclaimed to his social media audience that like this operation all subsequent US operations against Iran failed until 2015, when the nuclear deal was signed: "The Americans, from that year on, failed in every operation against Iran...until the year 1394 [2015] when they took revenge from us for all of their defeats with the JCPOA".[455] According to Yaminpour, the JCPOA could be the beginning of US victories over Iran unless principlists turned back the page and prevented Rouhani from being re-elected in 2017 election.

Yaminpour has also criticized Rouhani's moderate foreign policy in the Middle East, calling for a more military interventionist approach. For instance, he took a harsh tone against the Kingdom of Bahrain for the arrest of the prominent Shia cleric Sheikh Isa Qassim. He quoted Major General Ghasem Soleimini, the commander of the Quds Force of the Islamic Revolutionary Guard Corps (IRGC-QF) in charge of foreign operations, who set the arrest of Sheikh Issa as a red line. Yaminpour explained to his followers that "Violation of the sanctum of Ayatollah Sheikh Isa Ghasem is a red line that, if crossed, will spark a flame in Bahrain and the entire region and will leave nothing but armed resistance for the people."[456] Yaminpor asks whether the Iranian government will stand by this red line, and thus maintain its "position of leadership of the liberation movements of the world" or, as he implies is likely with Rouhani, it will simply give an ineffective diplomatic reply. An analysis of Yaminpour's posts shows a strong criticism of moderate politicians who advocate against Iranian arms buildup, in contrast to Zibakalam and Khatami. In an interview conducted by Yaminpour with IRGC Navy commander Commodore

---

[455] Yaminpour, Vahid. *Instagram*, 24 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTR1evpj1WX>.

[456] Yaminpour, Vahid. *Telegram*, 23 May 2017. Web. 02 Sept 2017. <https://t.me/yaminpour/698>.

Ali Fadavi, shared on social media, the latter told Yaminpour those in favor of diplomacy and negotiations were ignorant because what gave Iran the ability to conduct diplomacy and negotiate in the first place was its military power. Yaminpour responded by quoting a speech from Iranian Minister of Foreign Affairs Javad Zarif in which he said that the real strength of Iran flowed from the soft power generated by its revolution and not its hard military power, because all of the latter could be destroyed by the US with a single bomb. Yaminpour acerbically asked Fadavi what one could expect of people who said such things.[457] In supporting Iranian military interventionism and arms buildup, Yaminpour also celebrated the IRGC missile strike against ISIL and, in a veiled warning to Israel, said "The distance between the ISIL mosquitos with the Israeli flies is not much. It is as much as for the commander to say a few degrees higher."[458]

In the context of Iranian domestic politics, Yaminpour predictably focuses on social and economic issues, but from a conservative perspective. One such issue has been the United Nations 2030 Agenda for Sustainable Development (UN 2030) which calls for greater sexual education in schools and elimination of any and all discrimination against school children based on sexual orientation.[459] Ayatollah Khamenei has criticized Rouhani for allegedly implementing this in Iran, which created a big controversy among Iranian conservatives. The Iranian president has stated that this is not the case and that Iran has implemented UN 2030 selectively as it sees

---

[457] Yaminpour, Vahid. *Instagram*, 01 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTlDrA7gV8z>.

[458] Yaminpour, Vahid. *Instagram*, 18 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVfmtwJlL5K>.

[459] UNESCO. "Education 2030: Incheon Declaration and Framework for Action for the Implementation of Sustainable Development Goal 4." *The United Nations Educational, Scientific and Cultural Organization*, 2016, unesdoc.unesco.org/images/0024/002456/245656E.pdf>.

fit, meaning it has not implemented parts that it disagrees with. Yaminpour's social media discourse has used the experience of the JCPOA to argue that Rouhani's letters and plans may be deceitful or simply wrong, asserting "The experience of the JPCOA shows us what will befall us with the 2030 document is much worse than what has been said in the letters and plans" of the Rouhani administration. He has also painted the implementation of UN 2030 in Iran as the re-admission of neo-colonialism by Rouhani, contrasting it to the Iranian experience with nationalization of the oil industry: "65 years after the oil industry was nationalized, we want to sign a contract with UNESCO on our cultural and educational regime! This is the same neo-colonialism of which some sought proof."[460]

He has also been a harsh critic of the economic policies of the Rouhani administration and lavish and luxurious lifestyles of the Iranian elite. Yaminpour frequently quotes Ayatollah Ruhollah Khomeini in his posts to oppose the lavish lifestyles he claims are lived and propagated by some Iranian government officials while many Iranians live in poverty.[461] He used an image of a visit by Rouhani to the site of a mining accident, during which tired and disheveled looking miners threw rocks at the Iranian president's vehicle, to tell his social media followers that this is what happened "When the downtrodden do not believe the sympathy of rulers." He contended that the Rouhani administration's right-wing economic policies are catastrophic for social justice and "do not only make the poor and laborers hate them; the right-wing are the pests of the legitimacy of the regime and social solidarity." According to Yaminpour, this image is "one of the worst and most shameful images" that the world has seen of "the revolution of the downtrodden and

---

[460] Yaminpour, Vahid. *Telegram*, 30 May 2017. Web. 02 Sept 2017. <https://t.me/yaminpour/712>.

[461] Yaminpour, Vahid. *Instagram*, 12 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT_Kpk_gaYf>.

barefoot," drawing on the phrasing of Ayatollah Khomeini to characterize the Iranian Revolution.[462] He similarly intervened in the public debate about social inequality and class during the 2017 election, in which principlist candidates campaigned on a platform that claimed to put the "96 percent", or the majority of Iranians, against the "4 percent", or the narrow elite they argued benefited from the Rouhani administration's policies. Posting a picture of youth in Tehran in a luxury vehicle carrying a sign that said "The 4 percent is greater than the 96 percent", Yaminpour told his followers that many "Khorramshahrs" were on the way.[463] This is a reference to the Iranian liberation of the city of Khorramshahr from Iraqi occupation during the Iran-Iraq War, an important event in the history of the Islamic Republic. He boasted that after the reconquest of Khorramshahr, combating the lavish and luxurious lifestyle in Iran was another battle that needs to be won.

6.1.4. Hamid Rasaee

Hamid Rasaee is a principlist public figure who heads the conservative 9 Dey weekly newspaper, a former member of parliament, and a major critic of the moderates and reformists in Iran. He was among the critics of the JCPOA, and ultimately voted against it while in parliament. A survey of Rasaee's social media discourse shows the continuation of his critique of JCPOA and challenging the idea that it ended the economic sanctions regime against Iran and would be an impediment to its reconstruction. Rasaee has argued that, having successfully used sanctions to force Iran to concede in the JCPOA, the US and its allies would be tempted to reconstruct sanctions around another issue, such as Iran's ballistic missile industry, alleged support for

---

[462] Yaminpour, Vahid. *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTy3h6jgR4g>.

[463] Yaminpour, Vahid. *Telegram*, 23 May 2017. Web. 02 Sept 2017. <https://t.me/yaminpour/699>.

terrorism, or human rights. He warned if Rouhani was re-elected in the 2017 presidential election, "we must expect that the actualization of the demands of Westerners in areas of destruction of the missile industry, end of support for revolutionary groups of the region, and drawing of threats from within Lebanon and Syria to within Iran and acceptance of their demands on the human rights issue."[464] The post-JCPOA sanctions, such as the Countering Iran's Destabilizing Activities Act introduced in the US Senate on 23 March 2017, which Rasaee calls the "mother of all sanctions", was a fulfillment of what he had been saying about the reconstruction of sanctions around non-nuclear issues to curtail Iran's economy and trade.[465]

Like Yaminpour, an analysis of Rasaee's social media discourse also reveals he is a proponent of Iranian military power as one of the primary means of dealing with the regional and international issues facing the Islamic Republic. Like other princplists, he used the existence and actions of ISIL to defend a confrontational foreign policy and the use of military strength over a moderate foreign policy through diplomacy and negotiation. Immediately after the ISIL attacks in Tehran, Rasaee asserted:

> Now they know that the world of today is not the world of dialogue, now they found out that decreasing the defense budget and military and security forces is treason. Now they understand how reasonable and correct adopting the policy of 'engaging the enemy hundreds of kilometers from the soil of the country' is. Now they understand that the support of the regime for Hezbollah and presence in Iraq and Syria is so that today we do not have this worry, anxiety and fear.[466]

---

[464] Rasaee, Hamid. *Telegram*, 23 May 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4404>.

[465] Rasaee, Hamid. *Telegram*, 01 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4404>. and, Rasaee, Hamid. *Telegram*, 17 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4838>. and, Rasaee, Hamid. *Instagram*. Web. 02 Sept 2017. 19 June 2017, <https://www.instagram.com/p/BVg9LL_g5qZ>.

[466] Rasaee, Hamid. *Instagram*, 07 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVDi6hhDo7q>.

Following the retaliating IRGC missile strike against ISIL, Rasaee was quick to compare the results of principlists' military approach favorably with Rouhani's diplomatic approach, arguing the "fruit" of the military has been missiles while the fruit of diplomacy has been the "bitter" and "foul smelling" JCPOA, in that Western sanctions and insults have not decreased but only increased: "The fruit of missiles is not only not foul smelling but has a good scent, it is the cause of pride and honor."[467]

A reading of Rasaee's social media discourse also highlights that he, along with his 9 Dey weekly newspaper, were pioneers in creating the UN 2030 controversy and bringing it into the spotlight in the context of the 2017 election. Rasaee put great emphasis on the way the UN 2030 educational document negatively impacts the "culture of jihad and martyrdom" in Iran from the perspective of Iranian principlists. Rasaee argues UN 2030 educational reforms in Iran have allegedly removed jihadi and martyrdom subjects from elementary school textbooks, like the story of Hossein Fahmideh, a 13 year old who was killed after he detonated himself underneath an enemy tank during the Iran-Iraq War.[468] Rasaee similarly reports on rumors of the elimination of the IRGC-affiliated Youth Basij organization and "Preparation for Defense" basic military training course for high school boys. On a similar track, 13 Aban, Students Day in Iran commemorating the killing of students during the Iranian Revolution of 1979 in front of the University of Tehran, has been removed from the teaching of the history of the revolution.[469] Rasaee frames his objection to these policies with a quote from Iranian Supreme Leader Ayatollah Ali Khamenei: "This is the Islamic Republic and in this country the basis is Islam and

---

[467] Rasaee, Hamid. *Telegram*, 19 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4854>.

[468] Rasaee, Hamid. *Telegram*, 15 May 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4453>.

[469] Rasaee, Hamid. *Telegram*, 30 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4926>.

the Quran. This is not a place where the ill and defective and corrupting Western lifestyle can infiltrate. In the regime of the Islamic Republic acceptance of such a document has no meaning."[470] Rasaee similarly quotes a number of senior Iranian clergymen, including one who calls allowing the infiltration of Western culture and values in Iran as "war against the Imam of Time" which, in the context of the Iranian legal system and Shi'a political jurisprudence, is considered a crime so grave so as to require the death penalty.[471]

Rasaee has also weighed in on the important debate around the source of legitimacy in Islamic government in his social media discourse, a key political ideal of the Islamic Republic. One side of this debate, represented by Rouhani and the moderates, is that the legitimacy of the Islamic government is based on the votes and will of the people. In a recent speech, Rouhani quoted Ali ibn Abi Taleb, the first imam of Shi'a Islam, as having said that he followed the will of the people, so much so that anyone who the people elected would also become his own leader. Drawing on this historical precedent, Rouhani declared: "The basis of the leadership and government from the perspective of Ali is the vote and opinion of the people."[472] Rouhani underscored that the idea of democratic accountability of the government was not a Western idea but Islamic: "The election that we today carry out in Iran and similarly the subject of the vote of the people, is not following the thoughts of the West and we do not follow the vote of the people as the gift of the post-Renaissance West, we possess a faith, ideology, and religion that the Commander of the Faithful Ali viewed to be based on the opinion, demands and votes of the people." Democracy, according to this view, is extracted from the traditions of Shia Islam and

---

[470] Rasaee, Hamid. *Telegram*, 25 May 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4637>.

[471] Ibid.

[472] Rouhani, Hassan. *Official Website of the President of the Islamic Republic of Iran*, 14 June 2017. Web. 02 Sept 2017. <http://www.president.ir/fa/99408>.

therefore in no way indebted to the West. Another perspective, which has authoritarian tendencies and is propagated by Rasaee and his fellow Principlists on social media, represents the legitimacy of Islamic government as deriving from God instead of the people. Under this conception of the Islamic government, people who oppose the will of the Islamic government, as manifested in the words and deeds of supreme leader, have committed a sin, rather than the leader needing to align with the will of the people.[473] The idea of a democratic supreme leadership is therefore rejected as Western and secular. In this debate, Rasaee has taken this second position, and in so doing has harshly attacked Rouhani and accused him of "illiteracy" and "superficiality", disseminating the views and opinions of 13 senior clergymen on social media to the effect that Rouhani's views have no basis in Shi'a political jurisprudence.[474]

As the qualitative analysis above has shown, political ideals such as the source of legitimacy of Islamic government, legitimacy of political institutions such as the Guardian Council (GC), and desirability of specific domestic and foreign policies, corresponding to the resources that undergird the co-optive power of the state, are hotly debated in Iranian cyberspace. This contestation has been done by the two opposing Iranian political currents, the moderates and principlists, with two examples of the most followed figures from each current given above. This section briefly undertakes a quantitative analysis of these figures' content generation and the user engagement they spawn using activeness, in terms of the number of posts, and engagement, measured by user response, as the metrics. On both Instagram and Telegram platforms the number of posts generated by the figures themselves, excluding "forwarded" posts from other

---

[473] Rasaee, Hamid. *Telegram*, 16 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4806>;

[474] Rasaee, Hamid. *Telegram*, 16 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4809>; Rasaee, Hamid. *Telegram*, 20 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4862>. and, Rasaee, Hamid. *Telegram*, 20 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4863>.

pages, corresponds to the metric for their activeness. In terms of the metric for the level of user engagement, however, there is a difference between the two platforms. On Instagram, the number of likes and comments each post generates corresponds to the metric for the level of user engagement for this social media platform. On Telegram, the number of views each post generates corresponds to the level of user engagement for this messaging application, as the content on this platform does not have "like" or "comment" functions. The leading content generator on Instagram of the four figures discussed above was Vahid Yaminpour, who had 122 posts in the three months under consideration, followed by Sadegh Zibakalam, Mohammad Khatami, and finally Hamid Rasaee, as shown by figure 6.7. However, when it came to engagement on Instagram, Zibakalam prevailed, with an average of 24,457 likes and comments spread over 87 posts, followed by Yaminpour, Khatami, and Rasaee, as shown by figure 6.8. This means that the selected principlist public figures hold a more successful online track record in terms of content generation on Instagram, while selected moderate public figures are more successful in terms of user engagement.

Figure 6.7: Level of Activity of Selected Public Figures on Instagram

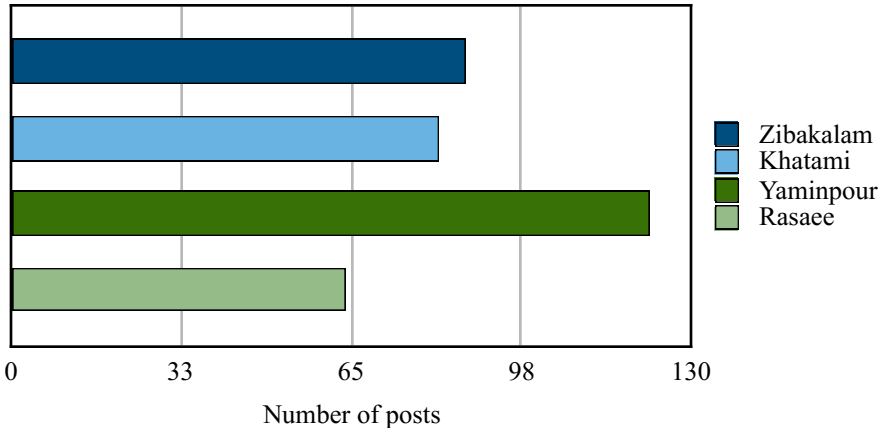
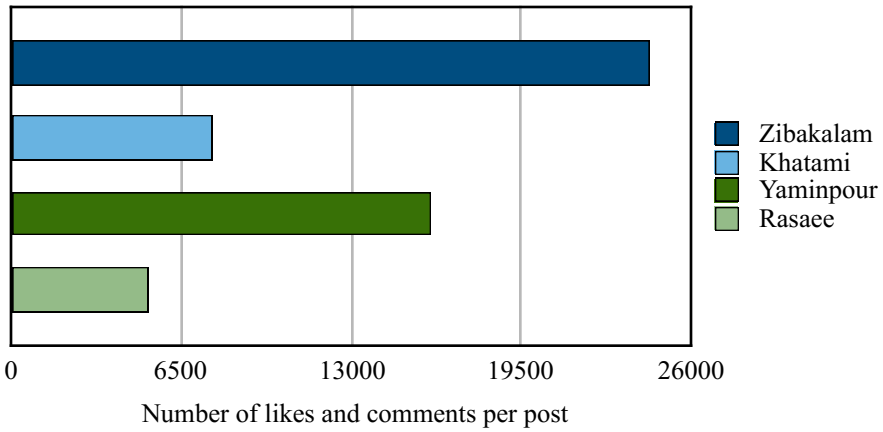


Figure 6.8: Level of User Engagement by Selected Public Figures on Instagram



The picture was slightly different on Telegram, where Rasaee was the most active with 541 posts, five times more than his nearest rival Yaminpour, followed by Zibakalam and Khatami, as shown by figure 6.9. However, Khatami's posts generated the most user engagement, totaling an average of 292,993 views per post, followed by Zibakalam, Yaminpour, and Rasaee, as shown by figure 6.10. Like Instagram, the greater level of content generation by the selected principlist public figures on Telegram does not necessarily correspond to greater engagement, and the selected moderate public figures hold a more successful online track record in this regard. It is interesting to note that while Iranian moderate social media figures and users often receive the most attention in the media, principlist figures and users are incredibly active on these platforms when it comes to generating posts. However the greater level of content generation by principlists, like Yaminpour and Rasaee, does not necessarily correspond to greater engagement. Figures 6.8 and 6.10, corresponding to user engagement on Instagram and Telegram respectively, show that moderates hold a more successful online track record in this regard.

Figure 6.9: Level of Activity of Selected Public Figures on Telegram

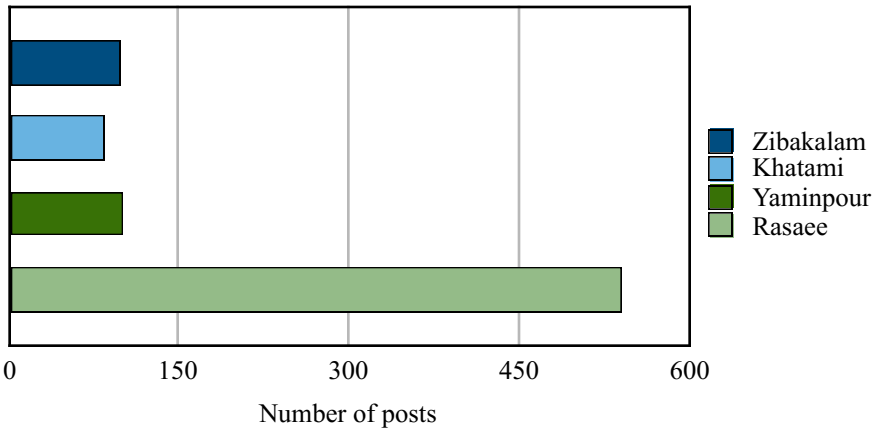
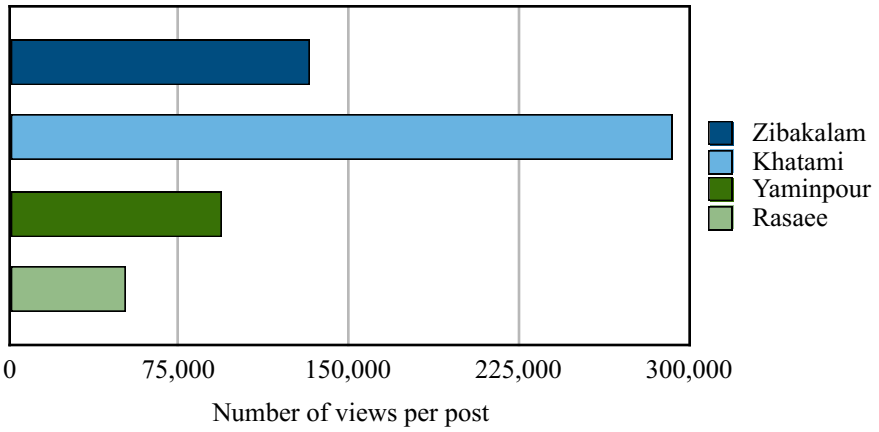


Figure 6.10: Level of User Engagement by Selected Public Figures on Telegram



6.2. Government Officials

The following four subsections will present the case studies of the top moderate and principlist government officials in the generation of ideational factors in Iranian cyberspace.

6.2.1. Hassan Rouhani

One of the most prominent government officials with a major online presence is moderate President Hassan Rouhani. Rouhani has used his cyber presence to counter the attempted online

hegemony of his principlist opponents. Cyberspace has been a primary domain through which Rouhani has attempted to defend the economic performance of his administration, which his opponents have accused of being unsuccessful and damaging to the poor. In series of social media posts, Rouhani defended his record by highlighting specific achievements. These included connecting the majority of villages in Iran to electricity, drinking water, and natural gas, providing universal healthcare for the first time, and making the country self-sufficient in strategic food commodities like wheat, all things that improved the daily lives of the poor.[475] He similarly underlined achievements when it comes to industrial infrastructure, including the aerial transportation sector and oil and gas industry, which prior to his administration and the JCPOA had been curtailed by international economic sanctions.[476] Rouhani responded in a strongly worded post to principlists who deny these achievements, comparing them to being "like Zionists, Wahhabis, and American hardliners, who are against the Iranian people" and the JCPOA. He further accused his hardline opponents of acting in line with American hawks, asserting that "When Trump came, they expressed happiness that he will tear up the JCPOA."[477] He attributes these opponents' anti-JCPOA stance to their ties with illicit trade and finance networks, which he labeled as "sanctions profit makers", who benefited from sanctions and lost economically after sanctions were lifted.[478]

---

[475] Rouhani, Hassan. *Instagram*, 08 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BSoZHKLlrZD>.

[476] Rouhani, Hassan. *Instagram*, 16 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BS9KIrPF1Om>. and, Rouhani, Hassan. *Instagram*, 01 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTithR9lzSP>. and, Rouhani, Hassan. *Instagram*, 02 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTl94CnlJrx>.

[477] Rouhani, Hassan. *Instagram*, 05 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTuTxucF3Kv>.

[478] Rouhani, Hassan. *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTzZWToFzwf>.

In foreign policy Rouhani's social media discourse shows that he challenges the military-centric view of his principlist opponents, instead arguing for a policy that balances military power and diplomacy. Rouhani challenged critiques that he has weakened the Iranian military by asserting that since the start of his presidency the military budget has increased by 77 percent.[479] He has also strongly defended the presence of Iranian troops in the Middle East and IRGC missile strikes against ISIL, but at the same time asserted that regional problems cannot be solved by military power alone, but require diplomacy, which proved its efficacy with the JCPOA. Rouhani explains that a foreign policy which overemphasizes military power is undesirable not only because it creates anxiety in other countries, but also because it leads to the securitization of Iranian society: "We are against those who want to create fear in the hearts of our people and people of the region. The power of Iran is for confronting against assault and we will stand against any kind of assaulter. However, we will not permit the continuation of your ill demeanor. You want to take freedom from the people and the people will stand against you. The period of violence has come to an end."[480]

Rouhani has also sought to advance the political ideals of the freedoms to access information and generate content in cyberspace. He has criticized principlist attempts to filter online content they consider undesirable, which Rouhani says they have done on the grounds that if social media access is not closed off "the whole people of Iran, will become irreligious and anti-revolutionary!"[481] He has argued instead that their real goal is to isolate Iranians "in the networks

---

[479] Rouhani, Hassan. *Telegram*, 15 Apr. 2017. Web. 02 Sept 2017. <https://t.me/president_iran/4249>.

[480] Rouhani, Hassan. *Instagram*, 08 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT27yYbFtWQ>.

[481] Rouhani, Hassan. *Instagram*, 15 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUH3nBWFxCc>.

they themselves have built," and he names the IRIB as one such network.[482] However, he contends that "The period when only one the IRIB would rule over people's opinions is over. By the further expansion of communications network infrastructure we shall make it so that every youth can be an IRIB with their mobile phone."[483]

During the 2017 Iranian presidential election, Rouhani used such issues to launch attacks against his principlist rival, Ebrahim Raisi, who had a background as a senior official in the judiciary, a key unelected political institution controlled by the principlists. When Raisi expressed openness to freedom of speech, Rouhani attacked him and the judiciary, saying "They speak of freedom of speech and critique...well! You who have cut tongues and sown mouths shut. Please do not speak of freedom, because freedom would be ashamed! Do not speak of critique. You work in an institution which no one dares critique."[484] The Iranian president proclaimed the people would reject Raisi and his cohort in the election because they would not "accept those who have only known how to execute and jail in the last 38 years."[485] Rouhani's critique of Raisi targeted the judiciary and reduced its entire record to "executions" and "jailing". He similarly went on the offensive against Friday prayer leaders, who are directly appointed by the supreme leader. Friday prayer leaders can often play an especially large role in local politics, like Raisi's father-in-law Ayatollah Ahmad Alamolhoda, who is a major voice in the important city of Mashhad in Khorasan Razavi province. Rouhani singled out Alamolhoda for criticism for his pronouncement

---

[482] Rouhani, Hassan. *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTzZWToFzwf>.

[483] Rouhani, Hassan. *Instagram*, 13 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUC0hwsFK6r>.

[484] Rouhani, Hassan. *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTzZWToFzwf>.

[485] Rouhani, Hassan. *Instagram*, 08 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT1rr7UFR1Q>.

that no one had a right to hold music concerts in his province because it was the sanctum of Imam Reza, a revered Shi'a figure whose shrine is located in Mashhad, and that anyone who wanted to hold a concert should leave the province. Rouhani excoriated Alamolhoda for his interference in governmental affairs, saying "You who want to govern the country, first tell us how you have governed Mashhad. Mashhad that was under your rule and continues to be; you told the people of Mashhad that if you want artistic programs leave Mashhad. Now you want to take over the country and tell the people to leave the country?"[486]

Finally, Rouhani has taken to social media to promote the political ideal of military non-interference in politics and the economy, especially when it comes to the Islamic Revolutionary Guard Corps (IRGC).[487] During a televised debate in the 2017 election, Rouhani called out the IRGC for its ballistic missile testing, revelation of its underground "missile cities", and writing of provocative anti-Israeli slogans on the side of missiles, which he claims were all done so they "could undermine the JCPOA with the creation of Iranophobia."[488] He has similarly expressed unhappiness with the economic role of the IRGC. Rouhani has specifically criticized the privatization process in the Islamic Republic, which was intended to hand over state assets to the private sector but ultimately handed many of these assets over to the IRGC: "The economy was in the hand of a government without guns and we took and gave them to a government with guns." This was problematic because the private sector, already afraid of the civilian "government without guns", now faced the troubling question of how to compete with the IRGC

---

[486] Rouhani, Hassan. *Instagram*, 17 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUNRauTFzbf>.

[487] Ibid.

[488] Rouhani, Hassan. *Instagram*, 05 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTuTxucF3Kv>.

"government with guns".[489] Rouhani claims that this has not only hurt the private sector and curtailed economic activity, but also distracts the military from its core security mission. He cited the Ayatollah Ruhollah Khomeini's last will and testament which explicitly stated that the armed forces should not interfere in politics and always keep a distance from political affairs.[490]

6.2.2. Ali Motahari

Ali Motahari is the deputy leader of the Iranian parliament and a maverick politician who supports the moderate policies of President Hassan Rouhani. He has been outspoken on social media when it comes to the political ideal of separation of powers between elected institutions, such as the presidential administration, and unelected institutions that principlists control, such as the judiciary. A review of Motahari's social media activities reveals that he has discussed this issue in a number of different contexts, including the house arrest of the leaders of the Green Movement, which is ongoing as of the time of writing. Green Movement supporters, who are unhappy with the house arrest and have demanded the release of the Green Movement leaders, make up an important base for the successful 2013 election and 2017 re-election campaigns of Rouhani. These demands have been answered by the Iranian president with calls for greater political freedoms and promises to work toward the release of the Green Movement leaders in 2013 and 2017.

However, following the landslide 2017 re-election victory by Rouhani, the head of the judiciary Ayatollah Sadegh Larijani questioned his competency to do so, asking "who are you to end the

---

[489] Rouhani, Hassan. *Instagram*, 29 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BV6kB9PFO33>.

[490] Rouhani, Hassan. *Instagram*, 18 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTBcasml-2b>.

house arrest?"[491] Motahari responded to this comment in defense of the president almost as soon as it was published, writing a letter to Larijani that he also published online: "I declare that the president, according to Article 113 of the Constitution, is responsible for implementing the Constitution, and when an action like house arrest is against article 32 to 37 of the Constitution, is duty-bound to take action in defense of the citizen rights of the nation, especially since the slogans of the people in the recent election showed that this issue is the desire of the majority of the people of Iran."[492] Motahari reiterated that Larijani's questioning of Rouhani's pledge was inappropriate given that the re-elected president has received 24 million votes. Even if house arrest had been the decision of the Iranian Supreme National Security Council (SNSC) under former President Mahmoud Ahmadinejad, as Larijani pointed out, Motahari noted that Rouhani, as the current head of the SNSC, was empowered by popular demand to reverse this decision. Larijani had also stated that even were the SNSC to reverse its decision, the judiciary would step in to prosecute the Green Movement leaders. However, Motahari questioned the right of the judiciary to do this. Addressing Larijani, he said: "It is interesting that in fact you are saying the judiciary, after the punishment of seven years house arrest, which is worse than imprisonment, can turn around and prosecute the accused to find out what their punishment is. I ask you, please do not repeat this. It is slander against the Islamic Republic."[493]

In order to challenge principlists, Motahari has not merely relied on propagating the political ideal of separation of powers between unelected institutions that principlists control such as the

---

[491] Esfandiari, Golnaz. "The Challenges Iranian President Rohani Faces In His New Term." *Radio Free Europe/ Radio Liberty*, 5 Aug. 2017. Web. 02 Sept 2017. <https://www.rferl.org/a/28660225.html>.

[492] Motahari, Ali. *Telegram*, 01 June 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/605.

[493] Ibid.

judiciary and elected institutions, such as the presidential administration. Motahari is also a staunch critic of policies promoted by the principlists. A careful look at his social media discourse shows some parallels with Zibakalam and Khatami. For example, in the area of economic policy he has been among the most staunch critics of the Ahmadinejad administration, and principlists more broadly, for their populism. He has been a particular critic of the Subsidy Plan, characterizing it as a "ruinous" plan with catastrophic consequences for the Iranian economy. He critiqued the 2017 presidential campaigns of principlist candidates Ebrahim Raisi and Mohammad-Bagher Ghalibaf along the same economic policy lines and accused them of wanting to run on this catastrophic legacy.[494] He leveled the particular charge that these principlist candidates would use any "illegitimate means", such as multiplying the cash disbursed by the Subsidy Plan, to reach victory. This is was while the Rouhani administration already had a 17 trillion toman deficit due to the funding requirements of the Support Plan, and there were no resources for principlists to fund their promises except to cut from other social services, which would place even greater pressure on the poor.

Motahari's social media discourse on foreign policy strongly backs Rouhani and the JCPOA. He told his followers that following the rise of the Donald Trump administration in the US, Iranian principlists had found an excuse to advance their confrontational foreign policy. Referring to them, he said that "Some do not fear that the JCPOA will be stillborn and, for the preservation of a revolutionary gesture, drag the country into an unwanted war."[495] While he supports the Iranian military presence abroad, he distinguished himself from principlists by saying that Iranian

---

[494] Motahari, Ali. *Instagram*, 13 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUC8XsZhk-Q>.

[495] Motahari, Ali. *Telegram*, 13 May 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/583>.

foreign policy in the Middle East must not create anxiety among the people of the region: "Iran must improve its relations with the Arab nations of the region, so that they do not take refuge with America and Israel, because unfortunately these countries have a phobia of Iran that we must ameliorate."[496]

His social media posts have also targeted the absolutely negative view of the principlists regarding international institutions, which they view as tools of the major powers, particularly in the context of the debate over the UN 2030 document, discussed in the sections on Yaminpour and Rasaee. This document is from UNESCO, an organization Motahari labelled as independent, reminding principlists that if this organization was under the influence of the major powers and not independent, it would not have defended and recognized Palestine, a cause principlists strongly support. He asserted that: "In fact, the question is whether or not we should have relations with international institutions? If we should not have relations with UNESCO then we should not have relations with the United Nations as well."[497]

In the realm of domestic politics, he told his social media followers that principlist policies would lead to the violation of citizen rights by unelected institutions that principlists control: "If a candidate other than Mr. Rouhani wins, the undermining of the rights of the nation, and that which has manifested in chapter three of the Constitution, shall increase by some security and intelligence institutions and the judiciary".[498] The principlist objective of limiting rights in the country is not merely harmful to the people and country, according to Motahari, but also self-

---

[496] Motahari, Ali. *Instagram*, 23 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUcQDi_hFNR>.

[497] Motahari, Ali. *Telegram*, 27 June 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/623>.

[498] Motahari, Ali. *Instagram*, 13 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUC8XsZhk-Q>.

destructive for principlists themselves. He contended the principlists' favorite domestic policy is to express satisfaction with the status-quo, claim there is no room for any criticism whatsoever, and accuse anyone who dared raise critiques that they had questioned the very legitimacy of the Islamic Republic. He went on to tell principlists that:

> I say to them, as long as you unconsciously believe in a deterministic logic that in the regime of the Islamic Republic, whatever happens by the hands of the governing institutions is completely correct, or in other words what happens is what must happen and that which does not happen is what must not happen, and that all of actions of security and military institutions and the judiciary is correct, and if we critique we have weakened the regime. Yes, as long as you have such a mentality, you shall be defeated in different institutions, because the people do not like justification of dysfunction and oppression.[499]

6.2.3. Ali Khamenei

Supreme Leader Ayatollah Ali Khamenei has among the most active cyber presences and has the highest number of followers of any Iranian government official. He has developed a number of key cultural and political ideals and policies which have become guiding lights for principlist politicians and figures further down the line. Chief among them is the political ideal of the "resistance economy" as a solution to the economic issues faced by the IRI, emphasizing social justice and resilience against challenges from the global economy, such as sanctions. One of the economic issues Ayatollah Khamenei has highlighted is unemployment which, as he explains, can create a plethora of social ills such as drug addiction, corruption, and family problems, all of which can translate into dissatisfaction with the Islamic Republic.[500]

---

[499] Motahari, Ali. *Telegram*, 22 May 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/595>.

[500] Khamenei, Ali. *Instagram*, 10 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BStg3Pqh4I2>.

He has also tied economic issues with the rivalry with hostile states, who may want to use political dissatisfaction as a result these issues to "strike" the Islamic Republic. In this regard, he has said that economic threats are more severe than military threats and that the main conflict in Iran today is an economic war: "The real war is an economic war, the real war is the war of sanctions, the real war is in the arenas of work, activity and technology inside the country. This is the real war!"[501] This discourse was particularly manifested in the 2017 presidential election campaigns of principlist candidates Ebrahim Raisi and Mohammad-Bagher Ghalibaf who utilized this discourse as an instrument to exploit anxiety among voters and mobilize them against incumbent President Hassan Rouhani.

A key cultural ideal that Ayatollah Khamenei has articulated can be encapsulated here under the label of "resistance culture", or the desire to preserve authentic Iranian and Islamic culture in the face of globalization and spread of foreign, particularly Western, culture and lifestyles in the country. According to Ayatollah Khamenei, among the major ideals of resistance culture are "jihad" and "martyrdom", which are threatened by foreign cultural ideals, including those celebrated in the UN 2030 document.[502] Referring to UNESCO, the organization behind the document, he asked in one post: "For what reason does a so-called international organization, that is definitely under the influence of the big powers, have the right to make decisions for the nations of the world with different cultures."[503] In another post on this subject, he has stated that: "UNESCO here is an instrument and showcase; there are hands behind the United Nations that

---

[501] Khamenei, Ali. *Instagram*, 21 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTJ99sLBQUo>.

[502] Khamenei, Ali. *Telegram*, 24 May 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6054>.

[503] Khamenei, Ali. *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTyR3VwBeRu>.

are designing intellectual and cultural and practical systems for everything of the nations of the world. This is wrong and unsound. What right do they [the UN and its affiliate] have to give opinions about countries and their traditions and ideas that they must act like this or like that."[504]

Ayatollah Khamenei has told his online followers that the approval and implementation of the UN 2030 document in the IRI is against the independence of the country and is thus "absolutely not permitted".[505] Ayatollah Khamenei does not only view cultural threats as coming from abroad. He has also repeatedly highlighted the important role played by cyberspace as a conduit of cultural threats against the Islamic Republic: "Today is an avalanche of correct and incorrect assertions crashing on the head of our Internet users; incorrect information, false information, harmful information, pseudo-information...Why must we allow this to happen? Why must we allow those things to develop in the country that are against our values, against our core principles, against all of the fundamental parts and pieces of our national identity, by those who despise us."[506] He concludes cyberspace should not be allowed to become a domain free for enemies to act against Iranian cultural values and political ideals. Instead, cyberspace should be managed so this does not happen.

On foreign policy, Ayatollah Khamenei has undertaken an absolute defense of Iranian activities in the Middle East, namely of the "defenders of the shrine". This term denotes those who have deployed to Iraq and Syria to defend sacred Shi'a shrines, but is in fact just a euphemism for Iranian and non-Iranian military personnel deployed by the IRI for combat and advisory missions

---

[504] Khamenei, Ali. *Telegram*, 21 June 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6365>.

[505] Khamenei, Ali. *Instagram*, 02 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BU12qUcBPas>. and, Khamenei, Ali. *Telegram*, 07 June 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6215>.

[506] Khamenei, Ali. *Instagram*, 15 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVW-lS6hJD5>.

in service of its foreign and security policy goals. Following the attack by ISIL on Tehran, Ayatollah Khamenei told his social media followers that if the shrine defenders did not fight ISIL and other enemies beyond Iranian borders, there would be more disasters within the country, and the Islamic Republic would have to "fight the enemies of the Shi'a people in Iranian cities."[507] As with the resistance culture highlighted above, he has emphasized the cultural values of jihad and martyrdom, including by Iranian-backed transnational Shi'a fighters of Afghan, Pakistani, Iraqi, Lebanese, and other origins. He has especially lionized young shrine defenders, telling his online followers to look at "such strong motivation. Such bright faith, that this youth from Iran, from Afghanistan, from other countries sets off, decides to leave his young spouse, young child, and comfortable life behind, goes to a foreign country, on foreign soil, carries out jihad in the path of God and become martyred. Is this a small thing? Step-by-step the history of the Islamic Revolution has seen such history-making wonders; these are wonders."[508]

Ayatollah Khamenei has also defended the direct Iranian military presence, specifically by the IRGC Quds Force, and using this justification has emphasized the centrality of military power to the security and defense doctrine of the Islamic Republic. For instance in one post defending the role of the IRGC Quds Force in the Middle East, he strongly attacked the US for placing pressure on Iran to reduce the IRGC's role in the region. Ayatollah Khamenei asserted that Iran would resist such pressure, because the Quds Force is the crux of Iranian power in the region. He went on to say the US notion that "That the IRGC and Basij should not interfere and not participate in regional issues means do not enter your sources of power into the scene...We must act contrary to

---

[507] Khamenei, Ali. *Instagram*, 18 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVfqTf2BKNS>.

[508] Khamenei, Ali. *Instagram*, 01 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTjgNbkBWbc>.

this and must definitely enhance and strengthen our sources of military and security power."[509] Obliquely critiquing Rouhani's foreign policy, he stated that moderation in foreign policy is not necessarily a good thing and that sometimes a country had to act in a confrontational fashion. He criticized those who say that challenge and confrontation has costs. Ayatollah Khamenei said "collaboration", his term for cooperation by regional countries with the United States, also has costs, pointing for instance to the US-Saudi arms deal and the transfer of wealth it entailed. He concluded that: "Yes, confrontation has costs, but collaboration also has costs. You look at the Saudi government which, in order to collaborate with the new US President, is forced to spend half of its financial resources in service of American goals and according to its desires. Are these not costs? Collaboration also has costs. If confrontation is to be reasonable, if confrontation is based on logic, if it is with confidence, its costs are far less than collaboration."[510] He also labelled the JCPOA, as a form of US-Iran collaboration, albeit in a less harsh tone given that the deal was negotiated by Rouhani with his permission. Ayatollah Khamenei claimed Iran had trusted the US and entered into this collaboration with it, but had been damaged in the process because the US had not been committed to the JCPOA and imposed costs on Iran.[511] Through this discourse, Ayatollah Khamenei questioned what has been the single largest achievement of Rouhani's presidency that was reached through diplomatic cooperation rather than military confrontation.

---

[509] Khamenei, Ali. *Telegram*, 12 June 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6280>.

[510] Khamenei, Ali. *Instagram*, 06 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVAft5XB9sj>.

[511] Khamenei, Ali. *Instagram*, 16 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVZVGGBBuQ_>.

6.2.4. Ebrahim Raisi

The last government official studied in this analysis is the principlist Ebrahim Raisi. He is the custodian of the Astan Ghods Razavi, or Imam Reza Shrine Foundation (IRSF), one of the largest charitable foundations in the Islamic world, a member of the Assembly of Experts, and the runner up candidate in the 2017 Iranian presidential election. A political ideal that Raisi has most strongly espoused online is that of social justice, going as far as to say that "After monotheism, no issue in our religion has been elaborated on as much as justice".[512] During the 2017 presidential campaign, Raisi called himself and was called by others the "Seyyed of the Poor", the term "seyyed" denoting his lineage from the family of the Prophet Muhammad and physically distinguished by the black turban he wears.[513] He proclaimed "I am the representative of the weak and downtrodden classes whose voice is not heard."[514] In his campaign, he often brought every substantive policy debate back to the issue of the economic problems faced by the country and the political ideal of social justice. For example, during the discussion of the Rights of Citizens, a political ideal advocated by Rouhani to expand social and political freedom in Iran and attack their principlist opponents, Raisi reinterpreted this idea to fit his social justice discourse and counterattack Rouhani: "The rights of citizens of an unemployed person is to have a job and the rights of citizens of a poor is to have minimum living."[515] Rouhani has also come out against what he has labelled as the regressive social attitude and policies of Raisi and principlists, claiming for instance that "I know them [principlists] well; once in a session they

---

[512] Raisi, Ebrahim. *Telegram*, 28 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1258>.

[513] Raisi, Ebrahim. *Telegram*, 10 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1702>.

[514] Raisi, Ebrahim. *Telegram*, 12 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1734>.

[515] Raisi, Ebrahim. *Telegram*, 12 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1759>.

decided to raise a wall in Tehran's sidewalks and create men and women's sidewalks; just like they created of gender separation circular in their workplaces".[516] "They say we want to raise walls," Raisi responded to his social media followers. While he appeared to accepted this assertion, he inverted its implications by placing it in a social justice context, saying: "we shall raise a wall between those who pillage the public treasury and the people."[517]

In order to further emphasize the significance of his social justice political ideal, Raisi has presented the economic situation in Iran as being truly dire through a social media blitz during the election. He noted how the Gini coefficient in Iran had gone from 0.36 to 0.47, which indicates a widening of the gaps between social classes.[518] He has presented statistics that indicate 40 percent of university graduates and 30 percent of youths are unemployed, that 14 percent of the population (or 11 million people) live in sprawling urban slums under bad conditions, and that 50 percent of the country's industrial capacity remains unused.[519] Highlighting the plight of 11 million Iranian youths of marrying age, an important theme for the socially conservative principlists, Raisi noted that the existing facilities to support marriage, such as special loans for young married couples to set up their lives, were insufficient and that there was a waiting list of 500,000 people for such loans.[520] In order to overcome this perceived dire situation of the country's economy, Raisi proposed several populist economic policies during his

---

[516] Rouhani, Hassan. *Instagram*, 08 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT1rr7UFR1Q>.

[517] Raisi, Ebrahim. *Telegram*, 09 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1658>.

[518] Raisi, Ebrahim. *Instagram*, 28 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTbfC8yF2f6>.

[519] Raisi, Ebrahim. *Telegram*, 26 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1229>. and, Raisi, Ebrahim. *Telegram*, 28 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1254>. and, Raisi, Ebrahim. *Telegram*, 07 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1567>.

[520] Raisi, Ebrahim. *Telegram*, 02 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1436>.

campaign. These have included expansion of Subsidy Plan by tripling the cash handouts to Iranians in the bottom third of the income ladder and creating 1.5 million jobs a year, among others.[521] As noted in the sections on Khatami, Zibakalam, and Motahari, such policies have been roundly criticized by the moderate political camp as impractical and populist rhetoric merely designed to exploit the anxiety of poor voters and mobilize them in the 2017 campaign.

When it comes to policies in the realm of foreign policy, Raisi's social media discourse has closely aligned with those of other principlists discussed in this chapter. Following the ISIL terrorist attack on Tehran, Raisi published a post claiming ISIL had been formed "with the Green light of America, and Saudi arms,"[522] and yet elsewhere remarked that ISIL had attempted to disturb the security of Tehran "with Saudi money and the plan of the American arrogance".[523] As already explained, Zibakalam has sought to discredit such conspiracy theories through a series of six online videos in which he explained the origins and evolution of the ISIL. Like other principlists, Raisi has also emphasized the importance of Iranian and non-Iranian military personnel fighting under the banner of the IRI throughout the Middle East. He has come right out and said that "The Resistance Current in countries such as Syria, Yemen, Palestine, and Lebanon, is the strategic depth of the Islamic Republic."[524] In the same vein, he has championed the defenders of the shrine, arguing that Iran has deployed them to fight its enemies abroad so that it would not have fight them on its own streets. He has declared that "The martyrs of the defenders of the shrine must be held in high esteem, champions who should not be insulted by the words of

---

[521] Raisi, Ebrahim. *Telegram*, 24 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1187>.

[522] Raisi, Ebrahim. *Instagram*, 15 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVX6xF8FEt2>.

[523] Raisi, Ebrahim. *Instagram*, 15 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVhSdh4l4G5>.

[524] Raisi, Ebrahim. *Telegram*, 10 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1709>.

some," referring to moderate pundits who have questioned their deployment abroad.[525] Raisi goes on to say in this post that "If these dear ones were not there and did not sacrifice their lives for the defense of Islam, today the trenches for the defense of Islam would be in the Azadi Square of Tehran and Martyrs Square in Mashhad. God will not forgive this ungratefulness."[526]

He has placed similarly great emphasis on Iranian ballistic missile capabilities and targeted Rouhani for his criticism in the context of the 2017 election debates of IRGC revelations of their underground "missile cities". He responded to the Iranian president in a post, proclaiming that "The country has missiles so foreigners do not look askance at us. Today this missile is the subject of degradation and joking of these gentlemen. Our dear courageous men, opened the underground to say that we are capable and the enemy should not look askance at us."[527] Finally, in the duality between collaboration through diplomacy, advocated by moderates, and confrontation through military power, emphasized by principlists, Raisi has, unsurprisingly, sided with the latter. He sees "serious problems" with the JCPOA and the diplomacy behind it, saying while Iran has lived up to its commitments, the United States has not. Raisi has used the example of post-JCPOA sanctions by the US congress against Iran, which he views as proof that the United States is not living up to its end of the bargain.[528] He proclaimed in a post: "Mr. Rouhani promised that with the JCPOA sanctions would be lifted, however unfortunately nothing has happened in the lives and dinner tables of the people."[529] Elsewhere he has rhetorically asked: "Has there been an economic boom or a decline in the problem of unemployment? What benefit

---

[525] Raisi, Ebrahim. *Instagram*, 05 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BU-FPZ9F9tT>.

[526] Ibid.

[527] Raisi, Ebrahim. *Telegram*, 12 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1741>.

[528] Raisi, Ebrahim. *Telegram*, 10 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1709>.

[529] Raisi, Ebrahim. *Telegram*, 05 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1496>.

has the JCPOA had for the people?"[530] His answer, unsurprisingly, has been that the country has seen no improvement as a result of the JCPOA. He has used the analogy of the Palestinian struggle to highlight the utility of military power over diplomacy, saying "Negotiating tables for determining the destiny of Palestine are ineffective. It is the mujahideen of Palestine who shall determine the future of Palestine."[531]

As the qualitative analysis above has shown, political ideals, institutions, and policies are hotly debated in Iranian cyberspace by Iranian government officials associated with the two opposing Iranian political currents, the moderates and principlists. This contestation centers on debates over ideals such freedom of expression, access to information in cyberspace, non-interference of the military in politics and the economy, separation of powers, and social justice; political institutions such as the judiciary and the legitimacy of decisions made by these institutions; and specific domestic and foreign policies, corresponding to the resources that undergird the co-optive power of the state. This section briefly undertakes a quantitative analysis of content generation by these government officials and the user engagement they spawn.

The leading content generator of the four government officials discussed above on Instagram was Ayatollah Khamenei, who had 430 posts in the three months under consideration, followed by Ebrahim Raisi, Hassan Rouhani, and finally Ali Motahari, as shown by figure 6.11. However, when it came to user engagement on this platform, Rouhani prevailed, with an average of 192,250 likes and comments spread over 88 posts, followed by Khamenei, Motahari, and Raisi, as shown by figure 6.12. This means that the greater level of content generation by the selected

---

[530] Ibid

[531] Raisi, Ebrahim. *Telegram*, 05 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/2238>.

principlist government officials on Instagram does not necessarily correspond to greater engagement. The selected moderate government officials hold a more successful online track record in this regard.

Figure 6.11: Level of Activity of Selected Government Officials on Instagram

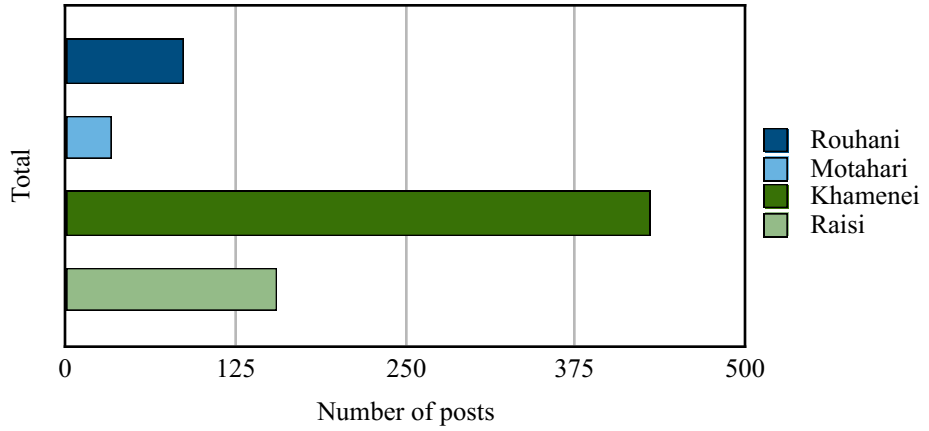
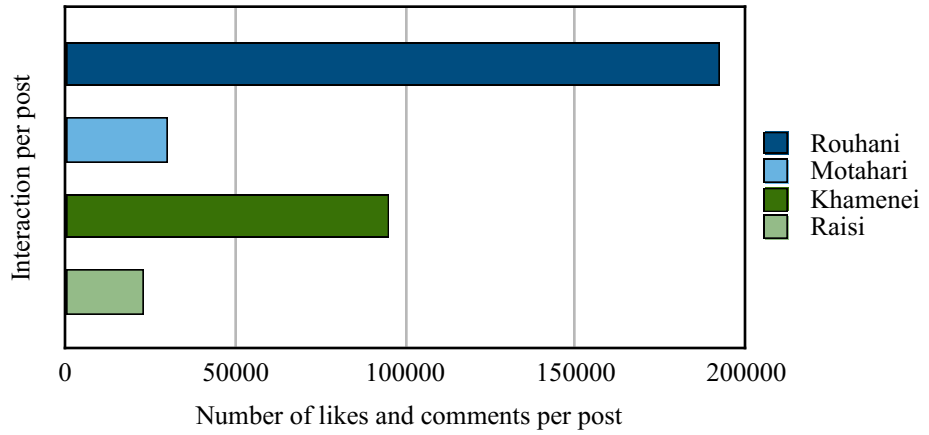


Figure 6.12: Level of User Engagement by Selected Government Officials on Instagram



The picture was different on Telegram, where Raisi was the most active with 1089 posts, followed by Rouhani, Khamenei, and finally Motahari, as shown by figure 6.13. In terms of user engagement, Khamenei's posts generated the most engagement, totaling an average of 675,182

views per post and nearly six times more than his nearest rival Raisi, and far outpacing Motahari, and Rouhani who followed in succession, as shown by figure 6.14. This means that the selected principlist government officials hold a more successful online track record on Telegram, both in terms of content generation and user engagement. As discussed previously, although moderate Iranian politicians often receive the most attention in the media based outside of Iran, principlist politicians are incredibly active on social media and often beat moderates, both in terms of generating posts and user engagement.

Figure 6.13: Level of Activity of Selected Government Officials on Telegram

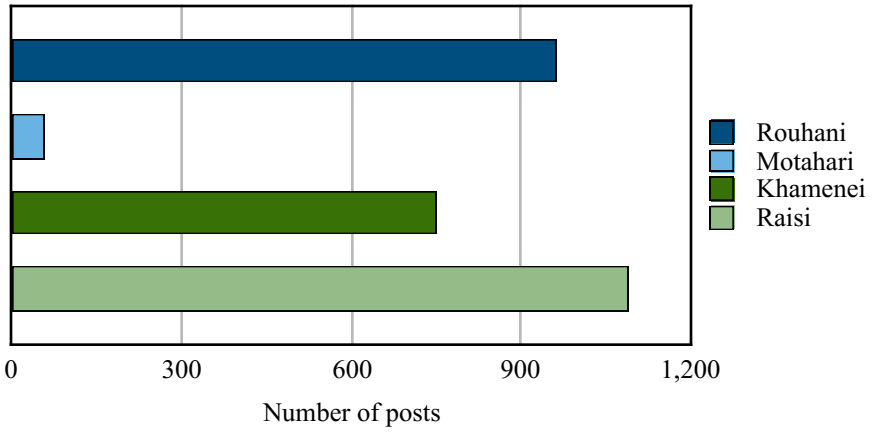
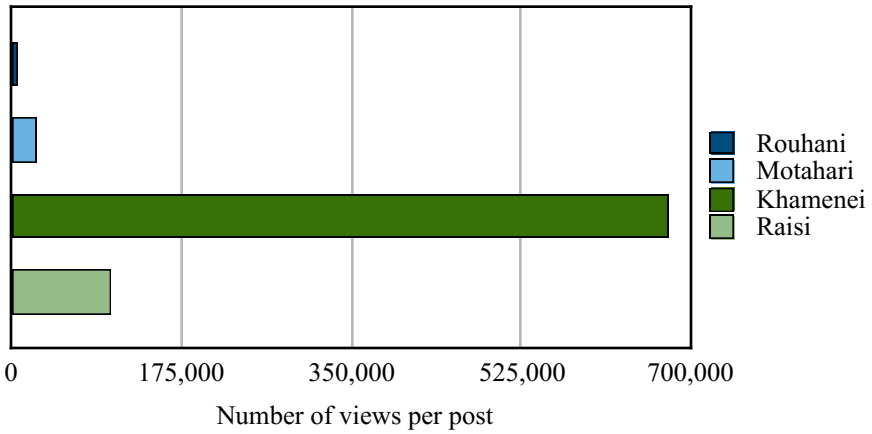


Figure 6.14: Level of User Engagement by Selected Government Officials on Telegram



Conclusion

This chapter analyzed co-optive power in Iranian cyberspace, generated from ideational sources such as political ideals, cultural values, the desirability of policies, and legitimacy of the role and track records of political institutions. In the initial step, the top domestic and foreign media outlet were selected and surveyed to identify the top Iranian public figures and government officials who generate these ideational factors in Iranian cyberspace. The side-findings of this initial step showed the top foreign media outlets, including BBC Persian and Manoto, had a larger audience on Instagram and Telegram, when compared to the top domestic media outlets such as Fars and Tasnim. This may be an indication that Iranian web users have greater trust in foreign rather than domestic outlets. The findings also show that foreign media outlets associated with the Iranian political opposition in exile had very little traction among Iranian web users when compared to other domestic and foreign outlets. This insight held true for figures associated with these exiled political opposition groups, with the exception of Reza Pahlavi, who had a large following, but was not included in the present study because he did not have a presence on Telegram until 11 May 2017, only part way through the period of this study.

The elimination of media outlets and figures associated with the Iranian political opposition in exile whittled the sample size down to cases of figures who can be considered to be within the framework of the Islamic Republic in one form or another. More specifically, the remaining sample was made up of public figures and government officials in the IRI establishment, evenly divided between the moderate and principlist political camps, the two main political groupings in the Islamic Republic. One interesting result of the quantitative analysis conducted on this data set

was the finding that, although moderate figures and officials often feature more frequently and prominently in the media, principlist figures and officials were actually very active online, although when compared to moderate figures and officials their track record was weaker when it came to user engagement. The qualitative analysis of the content generated by moderate figures and officials showed that they focused on the political ideals of socio-political freedoms, whereas principlist figures and officials emphasized the ideal of social justice. In the area of policies, accordingly, moderates advocated policies that enhanced socio-political freedoms, a more open and private-sector driven economy, and collaboration with other states in foreign policy. Principlists, in stark contrast, advocated policies that limited socio-political freedoms, promoted a more closed, redistributive, and state-driven economy, and a confrontational foreign policy. In terms of the legitimacy and track record of political institutions within the political structure of the Islamic Republic, the analysis shows that moderates and principlists defend elected and unelected institutions, respectively.

Besides the analysis and findings already discussed at length above, the present chapter has also made interesting findings on the critical question of how the Islamic Republic, and particularly the powerful principlist political current, approach cyberspace in regard to its potential co-optive power and the generation and distribution of ideational sources. Over the last two years, we have seen the IRI and principlist make the shift from a reactive to proactive approach to social media platforms in Iranian cyberspace. Under the reactive approach, cyberspace was viewed as a domain that could be mastered simply through the use of coercive measures, discussed in further detail in chapter three. There were two rationales behind this reactive approach. First, the limited distribution of technologies to access cyberspace in society, finite scale of the content produced

there, and availability of technologies to effectively filter content, convinced principlists that coercive measures were sufficient for managing cyberspace. Second, principlists lacked the wherewithal to engage in a competition over ideational factors with moderates and independent public intellectuals. The latter had historically exerted strong influence over the creation of attractive ideational factors in Iran, making competition seem futile for the principlists. Therefore, the ability to effectively block content in cyberspace and lack of confidence that attractive ideational factors could be produced became a mutually constitutive structure that pushed principlists to continue to emphasize a reactive approach to cyberspace.

However a shift in circumstances over the last few years has led principlists to move toward a more proactive approach to ideational factors in cyberspace that transcended exclusive use of coercion by also incorporating co-optive tools. First, it has become increasingly difficult, if not impossible, to effectively block content in cyberspace because of the ubiquity of means to access it and proliferation of online content. Second, principlists have become more confident in their ability to compete in the marketplace of ideological factors, thanks to the rise of a younger generation of savvy web users among them who are familiar with the weak and strong points of their own ideational factors as well as that of their moderate opponents. The relatively successful experience of the proactive approach by principlists on Instagram and Telegram has led some among them to attempt to join banned platforms such as Facebook and Twitter and recreate their success there. The more the proactive approach by principlists on these banned social media platforms makes the reactive approach obsolete, the more likely it is that the bans on them will be lifted in the future.

CONCLUSION

This dissertation has examined *the measures adopted by the Islamic Republic of Iran to manage the risks and opportunities presented by cyberspace as an emerging domain of power, and how these measures have interacted with Iranian state-society and international relations*. We began by observing that cyberspace is not merely a technological construct, but a phenomenon in which unprecedented level of social interaction takes place, and embedded within this, power relations have emerged which can impact both state-society and international relations. A debate continues to rage in the academic literature over the precise nature of this impact. In fact, the impact on state-society and international relations can vary depending on the context, which can be just as important as the core characteristics of cyberspace itself. This makes case studies a particularly useful research tool to tease out insights on how context shapes the political impact of cyberspace for a specific nation state. This dissertation therefore set out to conduct a case study of Iran which, despite experiencing the full spectrum of risks and opportunities associated with cyberspace, had hitherto not been studied in the necessary breadth or depth.

If cyberspace is indeed an emerging domain of power, we need a conceptualization of power in order to understand and explain power relations within it. Conventional definitions of power tend to focus on coercion and are state-centric. Such narrow conceptualizations are less useful for our purposes because they cannot subsume in themselves the different shades of power in cyberspace and the ways in which it impacts state-society and international relations. In this context, Robert W. Cox and Joseph S. Nye provide more comprehensive and nuanced conceptualizations of power that may be particularly useful for the purpose of this case study. These conceptualizations

go beyond coercion, focusing on consensus and the importance of ideational factors in creating consensus. Moreover, they are not state-centric, instead also looking at non-state actors such as international institutions, civil society organizations (CSOs), and the private sector. This dissertation drew on the four major dimensions of power as proposed by Cox and Nye. These are: coercive power, economic power, power embedded in international institutions, and co-optive power generated from ideational sources. Each of these dimensions in the context of Iranian cyberspace has been examined in chapters three through six by using a hybrid methodological toolbox suitable for analyzing quantitative and qualitative data collected from online public documents, academic literature on cyberpolitics, semi-structured interviews, raw technical and macro-economic data, and social media data. Below we summarize key insights from the dissertation on how cyberspace impacts state-society relations, followed by a glimpse at how it affects international relations.

As discussed at length in chapter one, cyberspace can impact state-society relations by reducing the costs of social mobilization. These costs are traditionally high, requiring hierarchical, bureaucratic, and capital and labour intensive organizations to recruit, communicate and coordinate a movements' participants. Instead, cyberspace enables social mobilization that is decentralized, low-cost, small, and not requiring the spatial and temporal co-presence of the movement's organizers and participants. Cyberspace can also enable fast and cheap fundraising by significantly reducing overhead costs, allowing for the efficient collecting of monetary sums mainly through the mass-collection of micro-contributions. Another mechanism through which cyberspace can facilitate social mobilization is the formation and enhancement of 'bridging social capital', related to resources available in weak ties (acquaintances), and 'bonding social

capital', related to the resources embedded in strong ties (family, close friends, and trusted associates). In the process of social mobilization, the complex web of weak ties in cyber networks works as an ideal tool for the circulation of information among a critical mass of citizens. Parallel to weak ties, strong ties within trusting networks of family and friends facilitate the sense of necessity and the possibility of collective action by providing strong emotional and substantive support for that action. Cyberspace can also impact state-society relations by optimizing and complementing tactics adopted by social movements, also known as 'repertoires of contention'. These can be divided to two main categories: cyber-assisted and cyber-based repertoires. In the first category, cyberspace enhances the efficiency of already available tactics by reducing the cost and increasing the speed, reach and size of collective action. For example, social movement organizations can use cyberspace to enhance fundraising and coordination for mobilizing national and transnational demonstrations. At another level, activists use cyberspace to develop new tactics enabled by and based within this domain, including online petitions and hactivism. Cyberspace can also impact state-society relations, particularly in countries where mass media is largely monopolized by the state, by generating and framing media coverage that challenges the state's ideological and hegemonic structures. In the process of generating and framing media coverage, social activists were historically dependent on corporate- or state-owned mass media, which would often show bias favoring authorities in power and established institutions and remain silent or distort activists' message. In the cyber era, however, social activists can leverage what Emanuel Castle calls 'mass self-communication', or the ability of the masses to self-generate and -direct messages to global audiences en masse. This leverage provides social activists with the opportunity to generate and frame media coverage by bypassing, indirectly accessing, and influencing mass media.

Many states have responded to these impacts of cyberspace by taking measures to limit its emancipatory potentials and maintain the status-quo in state-society relations in their own favor. In the case of the IRI, it has adopted three coercive measures. First is the National Information Network (NIN), a national intranet largely isolated from the global Internet. The NIN, which is almost without precedent in the world in its ambition, can be used by the IRI to limit access to the global Internet for Iranian society and compromise the cyber security of Iranian web users. The second is the comprehensive regime of filtering that coercively places barriers between the Iranian people and online content that the state does not want them to consume. This regime is among the most restrictive in the world alongside those of countries such as China. Finally, the Iranian body of law regulating cyber activities and the main law enforcement organizations for its implementation, are squarely aimed at deterring Iranians from cyber activities the IRI deems undesirable.

The IRI's deployment of these coercive measures are not wholly unique and can in many ways be viewed as serving a necessary function. Many countries utilize local intranets for government networks, universities and research centers, and private corporations. But rarely do countries utilize these networks as a substitute for the global Internet. In the same manner, many countries have filtering regimes and laws regulating cyber activities in order to block access to criminal content and prosecute online illegal activities or offline crimes facilitated by cyberspace, including the production and distribution of child pornography and illicit trafficking of arms, drugs, and humans. However, the utilization of these coercive measures by the IRI is problematic. The NIN, as a complement to the global Internet, can confer a number of benefits to Iranians and the IRI, including higher speeds and greater security from external attack. However, if the NIN is to be a substitute for the global Internet, and is thus used to isolate Iranians, it could

limit their ability to flourish through the Internet. The filtering regime and laws regulating cyber activities are typically deployed in the IRI as instruments to repress a wide range of online activity and content deemed to be against the system's religious and socio-cultural values and political ideals, rather than as scalpels to target undeniably criminal activity, as is the case in many other countries.

The IRI's use of these coercive measures is not simply problematic, but in the long-term may prove to be of limited effectiveness. For instance, if the IRI pursues the NIN as a substitute for the global Internet, this effort may eventually be made obsolete by advances in technology that make electro-magnetic wave Internet, namely through balloons and drones, globally ubiquitous. This would overcome the ability of the IRI to maintain a high degree of control over its Internet infrastructure, which today is mainly based on electrical or optical fiber cables in its territory. Moreover, despite the IRI's attempts to restrict and criminalize online content and activities, ordinary Iranians continue to consume content and engage in activities prohibited by the state on a large scale. This includes through circumvention as well as encryption and anonymization technology, which may simultaneously become more sophisticated and easier to use over time. Circumvention technology allows web users to overcome the filtering regime, while encryption and anonymization technology allow users to evade being identified and thereby escape criminal prosecution.

The limited effectiveness, and in some instances outright failure, of these coercive measures has led the IRI to make a shift from a reactive to proactive approach to Iranian cyberspace. Under the reactive approach, cyberspace was viewed as a domain that could be mastered simply through the use of coercive measures, based on two rationales. First, the limited distribution of

technologies to access cyberspace in society, finite scale of the content produced there, and availability of technologies to effectively filter content, convinced the IRI that coercive measures were sufficient to manage cyberspace. Second, IRI officials and public figures, particularly the principlists, lacked the wherewithal to engage in a competition over ideational factors with moderates and independent public intellectuals. However a shift in circumstances over the last few years has led principlists to move toward a more proactive approach to ideational factors in cyberspace that transcends exclusive use of coercion by also incorporating co-optive tools. First, it has become increasingly difficult to effectively block and criminalize content and activities in cyberspace. Second, principlists have become more confident in their ability to compete in the marketplace of ideas, thanks in part to the rise of a younger generation who are better able to generate and disseminate their favored ideas online.

An analysis of this proactive approach shows that, although moderates often feature more frequently and prominently in the media at home and abroad, principlists have become very active online in recent years in terms of promoting their favored political ideals, cultural values, policies and political institutions. When compared to moderates, however, principlists are weaker on user engagement. The qualitative analysis of online content generated by principlists illustrates that they focus on the political ideal of social justice, whereas moderates emphasize socio-political freedoms. On policies, principlists advocate policies that limit socio-political freedoms, promote a more closed, redistributive, and state-driven economy, and a confrontational foreign policy. Moderates, conversely, support policies that enhance socio-political freedoms, a more open and private-sector driven economy, and collaboration with other states in foreign policy.

Finally, when it comes to the legitimacy and track record of political institutions of the IRI, principlists and moderates are staunch supporters of unelected and elected institutions, respectively.

The impact of cyberspace goes beyond state-society relations to include international relations. Cyberspace can influence global politics through the new challenges it poses for international security, chief among them cyber espionage and sabotage. Cyberspace is extensively used by state and non-state actors for extracting sensitive and protected information for industrial espionage or obtaining government secrets. The most common form of industrial espionage through cyberspace is theft of proprietary information, especially intellectual property. This enables attacker to forgo the research and development costs associated with obtaining intellectual property and gain a competitive advantage by creating products more efficiently. Industrial espionage also gives the attacker leverage in negotiations or transactions by gaining insight into a victim organization's future plans. In the same vein, cyber espionage for the purpose of obtaining state secrets enables actors in global politics to better articulate their policies vis-a-vis their rivals in order to exploit their weakness.

Another, and more destructive, form of belligerent cyber operation is cyber sabotage, which can be used in tactical information operations and strategic attacks on critical infrastructure. The first type of cyber sabotage consists of actions for disrupting the information and communications systems on which a rival relies as a means of war. By changing the balance of information in a military context, the attacker conserves capital and labor to win the war. The second type of cyber sabotage consists of conducting strategic attacks on critical infrastructure. The Stuxnet worm, which targeted industrial systems underlying the Iranian nuclear program and specifically

its uranium enrichment infrastructure, is a prime example of the latter type of sabotage operation and made the IRI the first known victim of cyber sabotage posed by one state against another at the international level. Since the Stuxnet attack, the IRI has been victim of a number of other cyber espionage and sabotage operations including the Duqu and Flame malware.

These attacks made the IRI cognizant of the vulnerability of its industrial and ICT infrastructure to a wide range of cyber sabotage and espionage operations. As a result, the IRI founded the Cyber Defense Headquarters (CDH), which has taken several critical measures to protect Iranian ICT infrastructure against foreign cyber threats. In cyberspace, however, defensive measures alone are not sufficient to prevent rivals from conducting hostile cyber operations. Offensive measures are also necessary to demonstrate to rivals the capability to retaliate in case of an attack and thereby establish a deterrence relationship. To this end, the IRI has developed an offensive capability in the form of a designated unit called Cyber Offensive Headquarters (COH) to conduct such operations.

Following the formation of CDH and COH and implementation of their respective defensive and offensive measures, there has been no recorded significant cyber espionage and sabotage operation against the IRI's ICT infrastructure. This can be viewed as an indication of the successful record of CDH and COH in securing Iranian cyberspace and establishing deterrence over rivals. A second explanation may be that this resulted from decreased tensions between Iran and its rivals following resolution of the nuclear dispute in 2015, keeping in mind that the cyber operations against the country up to this point were mainly linked to the nuclear issue. It is important to note that while many countries utilize their cyber capabilities to defend and deter against cyber attacks

from rival states, the IRI also has a record of using these capabilities against online platforms used by Iranian civil society, domestic and foreign news websites, and major social network platforms such as Twitter, as the experience of the 2009 Green Movement demonstrates.

Cyberspace can also impact the power relations between states by providing a new domain for economic activities and competition. It can make a strong contribution to economic growth by fostering the diffusion of technology and innovation, enhancing the quality of economic and monetary decision-making, and increasing demand for and reducing costs of products. In the 2025 Horizon Vision Document, the IRI aimed to become the leading state among the 25 targeted countries in its immediate orbit in the areas of the economy, science, and technology in order to shift the regional balance of economic power in its favor. Developing information and communication technologies and exploiting their huge economic potential have been integral parts of the IRI's efforts to achieve this goal. Yet for all of the aspirations laid out in the document, actual progress in terms of exploiting ICTs for economic growth and development has been limited, uneven, and halting.

The IRI has achieved ICT infrastructure development rates close to the average of the 2025 Vision targeted countries. Iran's ICT infrastructure has continually developed since the early 2000s, with the exception of 2010-2011 period, when the Ahmadinejad administration imposed restrictions on ICT development during the Green Movement demonstrations. The Green Movement caused considerable alarm within the IRI, which sought to counter it through restrictions that stunted ICT infrastructure development during this period. Since this low point, the Rouhani administration has attempted to compensate for the underdevelopment inherited

from the past administration and made efforts to optimize infrastructure in order to reduce the cost of ICT services, manifested in the country's high scores for the ICT services affordability. This relatively satisfactory level of ICT infrastructure development, however, has not translated to a high level of effective utilization of ICTs in economic activities by citizens, the business sector, and government.

Among the highest indicator scores for ICT development in the IRI is the level of cyber literacy of its citizenry. The latter have acquired proficiency in the skills necessary for the utilization of novel cyber technologies, which is in turn crucial for optimal utilization of cyberspace for economic ends. Iranians have developed this level of skill because cyberspace has offered them a wide range of opportunities and advantages for both personal and professional use, including access to educational material and more efficient communications in a work setting. Moreover, the relatively closed media space in Iran has meant that cyberspace remains the main domain in which individuals have managed to find freedom of expression and access to information. Despite the high level of cyber literacy among Iranian citizens, however, the IRI's extensive filtering regime and restrictive penal code regulating cyber activities has impeded the full and effective utilization of cyberspace by individuals.

The Iranian business sector has experienced major impediments in terms of using ICTs and benefiting from their economic potentials. Among the main reasons behind this shortcoming is the domestic economic mismanagement and the confrontational foreign policy of the Ahmadinejad administration, which had a negative impact on all sectors of the economy, including those related Internet economy. Other barriers include excessive bureaucratic red-tape,

which has impeded business registration, a dearth of effective laws for regulating online business, and restrictive laws dealing with content generation and communication in cyberspace. The government lack of support for the business sector research and development (R&D) is yet another barrier in terms of the business sector's utilization and production of innovative technologies and progress towards a knowledge-intensive economy. Iran's relative isolation from the global economic system, as a result of sanctions, has also severely constrained the flow of capital, goods, and technology to Iran, stymieing ICT development. Following the Iran nuclear deal and the lifting of international sanctions, there is now a greater prospect for the private sector to play a crucial role in Iranian internet economy.

The government has also experienced difficulties in using ICTs to advance e-government development in Iran. The latter can help streamline and optimize the state bureaucracy, making government processes more efficient and cutting the cost of services provided by the government to the public. While Iranian governmental organizations seek to deploy ICTs to increase efficiency and reduce the cost of services, poor website design and slow Internet access speeds have impeded the effective utilization of ICTs by the public to access government information and services. Even where e-government has been implemented in the country to varying degrees, the digital divide in the country between developed and underdeveloped regions have troubling implications. This stark divide has led to the uneven actualization of economic benefits of e-government services.

Among the most challenging arenas where cyberspace can impact international relations is Internet Governance. The desire to exert control by state and non-state actors over cyberspace,

combined with the inherently global architecture of this space, have given rise to global institutions for Internet Governance. The decision-making and agenda setting embedded in these institutions in turn constitute one of main aspects of the exercise of power in cyberspace. In this context, the Internet Governance agenda presented by the IRI in global events since 2003 has been mainly preoccupied with three major issues. First, the IRI has emphasized that bridging the digital divide is the main requirement for realizing the huge potential of the Internet for economic development. It must be noted that the IRI emphasis on bridging the digital divide has been unevenly focused on the inequalities between states and actually obscured the inequalities within states. This is particularly the case for the IRI agenda under Ahmadinejad, which indicated that his administration prioritized the balance of economic power between states over empowering society, with the latter being relegated to an issue of secondary importance. Second, the IRI challenged the dominant role of Global North countries, particularly the United States, in controlling the critical Internet resources and called for all states to have an equal say in the management of these resources. Although the principlist administration of Mahmoud Ahmadinejad seemed to be more vocal in this regard, this was also pursued quite actively by the Mohammad Khatami and Hassan Rouhani administrations. Third, the role of non-state actors, such as the private sector and CSOs, in Internet Governance constitutes the main area of contention between different Iranian presidents. Contrary to the first and second issues, this one has revealed division between different Iranian presidential administrations. Ahmadinejad's government-centric agenda for Internet Governance sought to severely limit the role of non-state actors in order to enhance the hegemony of the state vis-à-vis society. Khatami and Rouhani, however, acknowledged the role of non-governmental organizations and were thus more open to the multi-stakeholder framework of Internet Governance.

The Ahmadinejad model for dealing with the role of non-state actors in Internet Governance seems unlikely to succeed in the long-term since non-state actors are key players in cyberspace. Much of the critical Internet resources and infrastructure is owned and managed by the private sector, meaning they are essential mediaries for states to take action in the cyber domain. This position within cyberspace has allowed the private sector to gain a voice in global forums, advance a multi-stakeholder agenda, and influence the outcome documents of these forums. In Iran, the globally oriented private sector has been weak as a result of economic sanctions and filtering of the Internet, and therefore had virtually no voice in cyber policy deliberations. With the lifting of international sanctions following the Iran nuclear deal, there is now a greater prospect for the globally-oriented private sector in Iran to blossom. Sanctions and filtering, however, have also created a nationally-oriented private sector with a perverse incentive to maintain a relatively closed cyberspace in Iran. Companies like DigiKala (valued at $150 million) and Aparat (valued at $30 million), Iranian versions of Amazon and YouTube, respectively, have popped up to fill the void left the international competitors. This nationally-oriented private sector has every incentive to maintain the status-quo. The IRI, in turn, may be able to call on the nationally-oriented private sector in the future to publicly support its sovereignist and restrictive global Internet governance agenda, allowing it to maintain a veneer of multi-stakeholderism.

Civil society organizations (CSOs) have also been active in promoting the protection of human rights in cyberspace. In contrast to the situation which is taking shape with the emergence of the nationally-oriented private sector, most of the CSOs in the country are beneficiaries of an open cyberspace which guarantees protection of human rights. The contributions of Tahmasebi and

Ebadi along with CSO representatives from other countries in Internet governance events demonstrate that the majority of genuine CSOs see a multi-stakeholder model of Internet governance as a key prerequisite for maintaining a free and open cyberspace. This means that if the IRI wants to maintain a semblance of support by Iranian CSOs behind its sovereigntist and government-centric agenda, it will likely have to fabricate these CSOs from scratch.

The overemphasis on the above three major issues has led the IRI to ignore the complexity of the emerging regime of global Internet Governance and, consequently, to overlook the increasingly pervasive phenomenon of transnational cybercrime. Although, this issue was raised by different stakeholders in several Internet Governance events, it was ultimately delegated to other international institutions. The international legal convention that has dealt with this issue first and most thoroughly is the Budapest Convention on Cybercrime, which has established a body of cybercrime law and a regime of cooperation to implement it, alongside an additional protocol in 2006 dealing with the distribution of racist and xenophobic material.

Despite having a comprehensive domestic regime of cybercrime law, Iran has neither addressed the issue of transnational cybercrime in Internet Governance forums nor joined international treaties such as Budapest Convention, leaving a gap in its laws when it comes to dealing with this growing problem. This appears to be because Iran has yet to deal with the kind of transnational cybercriminal activity on a large scale that has become prevalent in the developed world in recent years. Iran may also be concerned that joining international treaties such as Budapest Convention will create a conflict with its domestic cybercrime law and entail obligations which it is unwilling to undertake. However, as Iran's economy is gradually

reintegrated into the global economy following the lifting of international sanctions, and the Internet becomes more ubiquitous in the country, we may see a rise in transnational cybercrime affecting it and, as a consequence, an increased willingness on the IRI's part to add this issue to its global Internet Governance agenda.

A striking theme with relevance across all issue areas discussed above is the significance of non-state actors to the successful implementation of virtually all of the measures pursued by the IRI in cyberspace. The state, in and of itself, will no doubt continue to exert enormous influence in cyberspace, most obviously through coercion. However, even with this dimension of power in cyberspace, the IRI may not be able to successfully exercise power alone, instead requiring the cooperation, or at least acquiescence, of non-state actors, such as CSOs and the private sector. Take for instance, the National Information Network, which seeks both to enhance cybersecurity and prevent the entry of foreign ideational factors, including political ideas and cultural values, that the IRI deems as undesirable. The IRI will have difficulty achieving both of these objectives through coercion alone and without some level of cooperation with civil society and the private sector. As long as the service providers and users of the NIN do not acquiesce to and cooperate with the proscription of the ideational factors deemed as undesirable by the IRI, these factors are likely to continue to be generated and distributed within the NIN and Iranian cyberspace.

Similarly, weaknesses and vulnerabilities anywhere in the Iranian cyber eco-system, including in the private sector and society at large, could mitigate the utility of the NIN for cyber security. This basic logic also carries over to the IRI's filtering regime and cyber laws regulating online activities. The latter two are at best only somewhat effective because of the ambivalence of

society towards them. In many instances, the IRI's filtering regime and cyber laws are perceived as being overly broad by Iranian Internet users. In these instances, not only do users not cooperate with the IRI, but may actively work against it. In the cases of some cybercrimes, however, such as the production and distribution of child pornography and illicit trafficking of arms, drugs, and humans, society is amenable to cooperation with the state and can play an important role in helping the state prevent or address cybercrime.

The necessity of cooperating with non-state actors even extends to the realm of cyber defense and offense. The latter, almost exceptionally, is an area in which the state plays the central role. However, the experience of conflict since the 20th century has shown that the development of defensive and offensive capabilities often require the crucial input of the private sector and universities and research centers, among other entities. Without the mobilization of their knowledge, expertise, and productive capabilities, the creation of offensive and defensive capabilities would be rendered much more difficult. This is doubly true when it comes to cyberspace, where the state often does not possess the cutting edge knowledge and expertise necessary to innovate and develop novel capabilities needed to deal with adversaries.

Realizing the potential of the Internet economy is one area in which the power of the state is even more limited. While the state can facilitate the growth of the Internet economy through helpful regulations or removal of red-tape and is well positioned to implement e-government solutions to better deliver state services and save funds, it arguably plays a secondary role to the private sector. At the end of the day, it is the private sector around the globe that has played the main role in realizing the potential of the Internet economy. Large tech firms, such as Google,

Facebook, Amazon, Alibaba, among others, have created much of the basic hardware and software that forms the foundation of the Internet economy. Meanwhile, tech startups remain a key source of innovation, and increasingly the preponderance of offline sellers of goods and services have come online. Even when it comes to implementing e-government to reduce bureaucratic costs and optimize operations of service delivery to citizens, the state often relies on the private sector because the former lacks the technical capacity of the latter.

The discussion above also underlined the indispensable role played by non-state state actors in shaping the emerging global regime of Internet governance. States would be hard pressed to successfully formulate and implement Internet governance policy in the absence of the private sector, which owns and operates much of the infrastructure of cyberspace, and CSOs with expertise on key issue areas. The experience of Internet governance over the last several years has revealed that, in the absence of consensus between state and non-state actors, states are hard pressed to resolve even the simplest of issues. Conversely, when consensus between the two sides is forthcoming, even seemingly intractable issues can be resolved. The case of ICANN is illustrative in this regard: a coalition of state and non-state actors was able to come together to achieve the difficult goal of reducing the hegemonic role of the United States in the organization. To successfully pursue its Internet governance goals, therefore, the IRI needs to create an environment in which the private sector and CSOs that support its policies flourish.

Last but by no means least, the state by itself lacks the capacity to preserve the country's ideational factors in today's interconnected world, and instead must draw from civil society. This is a particularly acute point in the case of the IRI, which has exerted enormous coercive power to

prevent the influx of what it deems as harmful Western ideational factors. The reality, however, is that domestic ideational factors generated by Iranian social movements, Islamic and secular scholars and intellectuals, and progressive clergy in Islamic seminaries, among others, widely utilize cyberspace to critique the cultural and political ideals of the IRI. In other words if there is an ongoing contestation of ideational factors, it is largely between the IRI and Iranian civil society, rather than the IRI and its foreign adversaries. The IRI's highlighting of the West as the main source of this confrontation is arguably a tool used to paint its domestic critics as enemy agents. Nonetheless, the fear of cultural hegemony by outside forces is not limited to the IRI, but extends to many countries who have concerns about the preservation of their local ideational factors in an interconnected world. If the IRI has a genuine concern about this hegemony in cyberspace, it needs to permit a relatively open and free environment in which civil society can draw from the rich reservoir of pre-Islamic and Islamic Iranian culture and history to create local ideational factors that can counter those from abroad.

Cyberspace is the epicenter of an unprecedented level of interaction among a vast array of actors. Yet this novel domain, with the challenges it poses and benefits it endows, cannot be governed if the exclusive agent of this governance is to be the state, and its only tool coercion. Many countries have started with a state-centric and coercive approach toward cyberspace but, when the efficacy of this has proven illusory, have transitioned toward a more broad based approach. Such a transition is already underway in Iran and the future interplay of state-society and international relations will determine the trajectory of this evolution.

BIBLIOGRAPHY

English Sources

Abbate, Janet. *Inventing the Internet*. Cambridge, Mass: MIT Press, 1999.

Abdo, Geneive. "The New Political Tools." *The Iran Primer: Power, Politics, and U.S. Policy*. Ed. Robin B. Wright. Washington, D.C: United States Institute of Peace, 2011. 53-56.

Adib-Moghaddam, Arshin. *International Politics of the Persian Gulf: A Cultural Genealogy*. Abingdon: Routledge, 2009.

Adonis, Andrew, and Geoff Mulgan. "Back to Greece: The Scope for Direct Democracy." *Demos Quarterly* 3 (1994): 1-28.

Akhavan, Niki. *Electronic Iran: The Cultural Politics of an Online Evolution*. New Brunswick: Rutgers University Press, 2013.

Alberts, David S., and Daniel Papp S., eds. *The Information Age an Anthology on Its Impacts and Consequences*. Washington, D.C.: CCRP Publication Series, 1997.

Albright, David, Paul Brannan, and Christina Walrond. "Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report." *Institute for Science and International Security*. 15 Feb. 2011. Web. 01 Oct. 2017. <http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf>.

Alden, Christopher. "Let Them Eat Cyberspace: Africa, the G8 and the Digital Divide." *Millennium - Journal of International Studies* 32.3 (2003): 457-76.

Alexa. "parsijoo.ir Traffic Statistics." *Alexa*. 02 June 2017. Web. 02 June 2017. <http://www.alexa.com/siteinfo/parsijoo.ir>.

——. "Top Sites in Iran." *Alexa*. 02 June 2017. Web. 02 June 2017. <http://www.alexa.com/topsites/countries/IR>.

——. "yooz.ir Traffic Statistics." *Alexa*. 02 June 2017. Web. 02 June 2017. <http://www.alexa.com/siteinfo/yooz.ir>.

Alikhah, Fardin. "The Politics of Satellite Television in Iran." *Media, Culture and Society in Iran: Living with Globalization and the Islamic State*. Ed. Mehdi Semati. London: Routledge Taylor & Francis Group, 2010. 94-110.

Almeida, Virgilio A.f. "The Evolution of Internet Governance: Lessons Learned from NETmundial." *IEEE Internet Computing* 18.5 (2014): 65-69.

Andrés, Luis, David Cuberes, Mame Diouf, and Tomás Serebrisky. "The Diffusion of the Internet: A Cross-country Analysis." *Telecommunications Policy* 34.5-6 (2010): 323-40.

Ansari, Ali. *Iran, Islam and Democracy: the Politics of Managing Change*. London: Chatham House, 2006.

Antonopoulos, Christos, and Plutarchos Sakellaris. "The Contribution of Information and Communication Technology Investments to Greek Economic Growth: An Analytical Growth Accounting Framework." *Information Economics and Policy* 21.3 (2009): 171-91.

Aquilino, Broderick, Et al. *F-Secure Labs*. 2012. Web. 01 Oct. 2017. <https://www.f-secure.com/documents/996508/1030743/Threat_Report_H1_2012.pdf>.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" In *In Athena's Camp Preparing for Conflict in the Information Age*, by John Arquilla and David Ronfeldt, 23-60. Santa Monica: RAND Corporation, 1997.

Arquilla, John. "Twenty Years of Cyberwar." In *Military Ethics and Emerging Technologies*, by Timothy J. Demy, George R. Lucas, Jr., and Bradley J. Strawser, 275-82. New York: Routledge, 2014.

Asadzade, Peyman. "New Data Shed Light on the Dramatic Protests in Iran." *The Washington Post*. 12 Jan. 2018. Web. 05 May 2018. <https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/12/what-data-show-us-about-irans-protests/?utm_term>.

Bakshy, Eytan. "Rethinking Information Diversity in Networks." *Facebook*. 17 January 2012. Web. 01 August 2016. <https://www.facebook.com/notes/facebook-data-science/rethinking-information-diversity-in-networks/10150503499618859/>.

Ball, James. "GCHQ Captured Emails of Journalists from Top International Media." *The Guardian.* 19 Jan. 2015. Web. 07 Apr. 2018. <https://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post>.

Barraclough, Steven. "Satellite Television in Iran: Prohibition, Imitation and Reform." *Middle Eastern Studies* 37.3 (2001): 25-48.

Bátora, Jozef, and Iver Neumann B. "Cautious Surfers: The Norwegian Ministry of Foreign Affairs Negotiates the Wave of the Information Age." *Diplomacy & Statecraft* 13.3 (2002): 23-56.

Becker, Barbara, and Josef Wehner. "Electronic Networks and Civil Society: Reflections on Structural Changes in the Public Sphere." *Culture, Technology, Communication: Towards an Intercultural Global Village*. Ed. Charles Ess and Fay Sudweeks. Albany, NY: SUNY Press, 2001. 65-85.

Bell, Roderick, ed. *Political Power: A Reader in Theory and Research*. New York: Free Press, 1969.

Bennett, W. Lance, Christian Breunig, and Terri Givens. "Communication and Political Mobilization: Digital Media and the Organization of Anti-Iraq War Demonstrations in the U.S." *Political Communication* 25.3 (2008): 269-89.

Betz, David. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies* 35.5 (2012): 689-711.

Bimber, Bruce, Andrew J. Flanagin, and Cynthia Stohl. "Reconceptualizing Collective Action in the Contemporary Media Environment." *Communication Theory* 15.4 (2005): 365-88.

Bjola, Corneliu, and Lu Jiang. "Social Media and Public Diplomacy: A Comparative Analysis of the Digital Diplomatic Strategies of the EU, U.S. and Japan in China." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 71-88.

Bleha, Thomas. "Down to the Wire." *Foreign Affairs* 84.3 (2005): 111-17.

Branigan, Tania. "'Iranian' Hackers Paralyse Chinese Search Engine Baidu." *The Guardian*. 12 Jan. 2010. Web. 05 June 2017. <https://www.theguardian.com/technology/2010/jan/12/iranian-hackers-chinese-search-engine>.

Brock, Gerald W. *The Second Information Revolution*. Cambridge, MA: Harvard University Press, 2003.

Bronk, Christopher, and Eneken Tikk-Ringas. "The Cyber Attack on Saudi Aramco." *Survival* 55.2 (2013): 81–96.

Brunsting, Suzanne, and Tom Postmes. "Social Movement Participation in the Digital Age: Predicting Offline and Online Collective Action." *Small Group Research* 33.5 (2002): 525-54.

Brynjolfsson, Erik, and Adam Saunders. *Wired for Innovation: How Information Technology Is Reshaping the Economy*. Cambridge, MA: MIT Press, 2010.

Burnham, David. *The Rise of the Computer State*. New York: Random House, 1983.

Campbell, David. "Poststructuralism." *International Relations Theories: Discipline and Diversity.* Ed. Tim Dunne, Milja Kurki, and Steve Smith. Oxford: Oxford University Press, 2013. 213-37.

Castells, Manuel. *Communication Power*. Oxford: Oxford University Press, 2009.

——. *Information Technology, Globalization and Social Development*. Geneva: UNRISD, 1999.

——. *The Rise of the Network Society*. Oxford: Blackwell, 1996.

Carr, Edward Hallett. *The Twenty Years' Crisis, 1919-1939: An Introduction to the Study of International Relations.* London: Macmillan, 1946.

Cava-Ferreruela, Inmaculada, and Antonio Alabau-Muñoz. "Broadband Policy Assessment: A Cross-national Empirical Analysis." *Telecommunications Policy* 30.8-9 (2006): 445-63.

CE. "Chart of Signatures and Ratifications of Treaty 185." *Council of Europe*. 18 Dec. 2016. Web. 18 Dec. 2016. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=X4TZJpSX>.

Chase, Michael, and James Mulvenon C. You've Got Dissent!: Chinese Dissident Use of the Internet and Beijing's Counter-strategies. Santa Monica, CA: RAND, 2002.

Chawki, Mohamed. "Anonymity in Cyberspace: Finding the Balance between Privacy and Security." *International Journal of Technology Transfer and Commercialisation* 9.3 (2010): 183-99.

Choucri, Nazli, and Daniel Goldsmith. "Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security." *Bulletin of the Atomic Scientists* 68.2 (2012): 70-77.

Chowdary, T.h. "Diminishing the Digital Divide in India." *INFO* 4.6 (2002): 4-8.

CHRI. "Young Man Facing Death for Insulting Islam Online Tricked into Signing Confession."*Center for Human Rights in Iran*. 24 Mar. 2017. Web. 05 June 2017. <https://www.iranhumanrights.org/2017/03/young-man-facing-death-for-insulting-islam-online-tricked-into-signing-confession/>.

Clark, David, Thomas Berson, and Herbert Lin, eds. *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington, DC: National Academies, 2014.

Clark, Wesley K., and Peter L. Levin. "Securing the Information Highway." *Foreign Affairs* 88.6 (2009): 2-9.

Clarke, Amanda. "Business as Usual? An Evaluation of British and Canadian Digital Diplomacy as Policy Change." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 111-27.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The next Threat to National Security and What to Do about It*. New York, NY: Harper Collins, 2010.

Cleaver, Harry M. "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric." *Journal of International Affairs* 51.2 (1998): 621-40.

CNN. "Google's Eric Schmidt on Protecting America's Tech Secrets." *CNN*. 13 Dec. 2011. Web. 05 June 2017. <http://outfront.blogs.cnn.com/2011/12/13/googles-eric-schmidt-on-protecting-americas-tech-secrets/>.

Collins, Sean, and Stephen Mccombie. "Stuxnet: the Emergence of a New Cyber Weapon and Its Implications." *Journal of Policing, Intelligence and Counter Terrorism* 7.1 (2012): 80-91.

Comodo. "Comodo SSL Affiliate The Recent RA Compromise." *Comodo Blog*. Comodo, 23 Mar. 2011. Web. 05 June 2017. <https://blog.comodo.com/other/the-recent-ra-compromise/>.

Conroy, Meredith, Jessica T. Feezell, and Mario Guerrero. "Facebook and Political Engagement: A Study of Online Political Group Membership and Offline Political Engagement." *Computers in Human Behavior* 28.5 (2012): 1535-546.

Conway, Maura. "Terrorism and New Media: The Cyber-Battlespace." *Countering Terrorism and Insurgency in the 21st Century: International Perspectives*, Ed. James J. F. Forest, Vol. 2. Westport, CT: Praeger Security International, 2007. 363-84.

Copeland, Daryl. "Virtuality, Diplomacy, and the Foreign Ministry: Does Foreign Affairs and International Trade Canada Need a "V Tower"?" *Canadian Foreign Policy Journal* 15.2 (2009): 1-15.

Cordesman, Anthony H. *The Gulf Military Balance: The Conventional and Asymmetric Dimensions*. Washington, D.C.: Center for Strategic and International Studies, 2014.

Cox, Robert O. "Realism, Political Economy and the Future World." *New Diplomacy in the Post Cold War World: Essays for Susan Strange*. Ed. Susan Strange, Roger Morgan, Jochen Lorentzen, and Anna Leander. New York, NY: St. Martin's, 1993. 27-44.

Cox, Robert W. "Gramsci, Hegemony and International Relations : An Essay in Method."*Millennium: Journal of International Studies* 12.2 (1983): 162-75.

—— ed. *The New Realism: Perspectives on Multilateralism and World Orde*r. New York, NY: United Nations University Press, 1997.

——. *Production, Power, and World Order: Social Forces in the Making of History.* New York: Columbia University Press, 1987.

——. "Social Forces, States and World Orders: Beyond International Relations Theory." *Millennium: Journal of International Studies* 10.2 (1981): 126-55.

Cox, Robert W., and Timothy J. Sinclair. *Approaches to World Order*. Cambridge: Cambridge University Press, 2001.

Cull, Nicholas J. "The Long Road to Public Diplomacy 2.0: The Internet in US Public Diplomacy." *International Studies Review* 15.1 (2013): 123-39.

Dabashi, Hamid. *Iran, the Green Movement and the USA The Fox and the Paradox*. London: Zed, 2010.

De Bossey, Château. "Report of the Working Group on Internet Governance." *The Internet Governance Forum (IGF)*. June 2005. Web. 08 August 2016. <http://www.wgig.org/docs/WGIGREPORT.pdf>.

Dean, David, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'day, John Pineda, and Paul Zwillenberg. "The Internet Economy in the G-20." *The Boston Consulting Group (BCG)*. Mar. 2012. Web. 01 Mar. 2017. <https://www.bcg.com/documents/file100409.pdf>.

Deibert, Ronald. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart, 2013.

Deibert, Ronald, et al. "Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia-Georgia War." *Security Dialogue* 43.1 (2012): 3–24.

Deibert, Ronald, and Rafal Rohozinski. "Control and Subversion in Russian Cyberspace." *Access Controlled: the Shaping of Power, Rights, and Rule in Cyberspace*. Ed. Ronald Deibert et al. Cambridge, MA: MIT Press, 2010, 3–14.

——. "Liberation vs. Control: The Future of Cyberspace." *Journal of Democracy* 21.4 (2010): 43-57.

——. "Tracking GhostNet: Investigating a Cyber Espionage Network." *Information Warfare Monitor*. 29 March 2009. Web. 07 August 2016. <https://citizenlab.org/2009/03/tracking-ghostnet-investigating-a-cyber-espionage-network/>.

Deibert, Ronald, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010.

Della Porta, Donatella, and Mario Diani. *Social Movements: An Introduction*. 2nd ed. Malden, MA: Blackwell Publishing, 2006.

Deluca, Kevin M., Sean Lawson, and Ye Sun. "Occupy Wall Street on the Public Screens of Social Media: The Many Framings of the Birth of a Protest Movement." *Communication, Culture & Critique* 5.4 (2012): 483-509.

DeNardis, Laura. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.

Denning, Dorothy E. "A View of Cyberterrorism Five Years Later." *Internet Security: Hacking, Counterhacking, and Society*, Ed. Kenneth Einar. Himma. Sudbury, MA: Jones and Bartlett Publishers, 2007. 123-40.

Dewan, Sanjeev, and Frederick J. Riggins. "The Digital Divide: Current and Future Research Directions." *Journal of the Association for Information Systems* 6.12 (2005): 298-337.

DOJ. "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities." *The United States Department of Justice*. 24 Mar. 2016. Web. 05 June 2017. <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated>.

——. "United States of America Vs Ahmad Fathi; Hamid Firoozi; Amin Shokohi; Sadegh Ahmadzadegan, a/k/a Nitr0jen26; Omid Ghaffarinia, a/k/a Plus; Sina Keissar; And Nader Saedi, a/k/a Turk Server." *The United States Department of Justice.* 24 Mar. 2016. Web. 05 June 2017. <https://www.justice.gov/usao-sdny/file/835061/download>.

Drezner, Daniel W. "Weighing the Scales: The Internet's Effect On State-Society Relations." *The Global Flow of Information: Legal, Social, and Cultural Perspectives*. Ed. Ramesh Subramanian and Eddan Katz. New York: New York University Press, 2011. 121-38.

Dunn Cavelty, Myriam. "Critical Information Infrastructure: Vulnerabilities, Threats and Responses." *UNIDIR Disarmament Forum*.3 (2007): 15-22.

——. *Information Age Conflicts: A Study of the Information Revolution and a Changing Operating Environment*. Zurich: Center for Security Studies (CSS), 2002.

Eagleton-Pierce, Matthew. "The Internet and the Seattle WTO Protests." *Peace Review* 13.3 (2001): 331-37.

Earl, Jennifer. "Pursuing Social Change Online: The Use of Four Protest Tactics on the Internet." *Social Science Computer Review* 24.3 (2006): 362-77.

Earl, Jennifer, and Katrina Kimport. *Digitally Enabled Social Change: Activism in the Internet Age*. Cambridge, MA: MIT Press, 2011.

Ebadi, Shirin. "International Federation for Human Rights." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 16 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/tunis/scripts/archive.asp?lang=en&c_type=2|16&c_num=293>.

EIU. "The 2002 E-readiness Rankings." *The Economist Intelligence Unit*. 2002. Web. 01 Mar. 2017. <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010005.pdf>.

——. "The 2003 E-readiness Rankings." *The Economist Intelligence Unit*. 2003. Web. 01 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/eready_2003.pdf>.

——. "The 2004 E-readiness Rankings." *The Economist Intelligence Unit*. 2004. Web. 01 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/ERR2004.pdf>.

——. "The 2005 E-readiness Rankings." *The Economist Intelligence Unit*. 2005. Web. 01 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/2005Ereadiness_Ranking_WP.pdf>.

——. "The 2006 E-readiness Rankings." *The Economist Intelligence Unit*. 2006. Web. 01 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/2006Ereadiness_Ranking_WP.pdf>.

——. "The 2007 E-readiness Rankings: Raising the Bar." *The Economist Intelligence Unit*. 2007. Web. 01 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/2007Ereadiness_Ranking_WP.pdf>.

——. "Digital Economy Rankings 2010: Beyond E-readiness Economist." *The Economist Intelligence Unit.* 2010. Web. 01 Mar. 2017. <http://graphics.eiu.com/upload/EIU_Digital_economy_rankings_2010_FINAL_WEB.pdf>.

——. "E-readiness Rankings 2008: Maintaining Momentum." *The Economist Intelligence Unit*. 2008. Web. 01 Mar. 2017. <http://www-05.ibm.com/ie/pdf/ibm_ereadiness_2008.pdf >.

——. "E-readiness Rankings 2009: The Usage Imperative." *The Economist Intelligence Unit*. 2009. Web. 01 Mar. 2017. <http://graphics.eiu.com/pdf/E-readiness%20rankings.pdf>.

——. "The Economist Intelligence Unit / Pyramid Research E-readiness Rankings." *The Economist Intelligence Unit*. 2001. Web. 01 Mar. 2017. <https://web.archive.org/web/20071013015357/http://www.ladlass.com/ice/archives/files/E-Readiness_from_Economist%202001.pdf>.

——. "The EIU's E-business Readiness Rankings." *The Economist Intelligence Unit*. 2000. Web. 01 Mar. 2017. <https://web.archive.org/web/20011121105637/http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=3331&country_id=&title=The+EIU%27s+e-business+readiness+rankings,+May+2000&channelid=6&categoryid=20>.

Elin, Larry. "The Radicalization of Zeke Spier: How the Internet Contributes to Civic Engagement and New Forms of Social Capital." *Cyberactivism: Online Activism in Theory and Practice*, Ed. Martha McCaughey and Michael D. Ayers. New York: Routledge, 2003. 97-114.

Eloranta, Jari, Hossein Kermani, and Babak Rahimi. "Facebook Iran: Social Capital and the Iranian Social Media." *Social Media in Iran: Politics and Society after 2009*, Ed. David M. Faris and Babak Rahimi. Albany: State University of New York Press, 2015. 19-40.

Entman, Robert M. "Framing: Toward Clarification of a Fractured Paradigm." *Journal of Communication* 43.4 (1993): 51-58.

Esarey, Ashley, and Randy Kluver, eds. *The Internet in China: Cultural, Political, and Social Dimensions*. Great Barrington, MA: Berkshire Publishing Group, 2014.

Esfandiari, Golnaz. "The Challenges Iranian President Rohani Faces In His New Term." *Radio Free Europe/Radio Liberty*, 5 Aug. 2017, <https://www.rferl.org/a/28660225.html>.

Ess, Charles M. "The Political Computer: Democracy, CMC, and Habermas." *Philosophical Perspectives on Computer-Mediated Communication*. Ed. Charles M. Ess. Albany, NY: SUNY Press, 1996. 197-230.

Etzioni, Amitai. "Are Virtual and Democratic Communities Feasible?" *Democracy and New Media*. Ed. Henry Jenkins and David Thorburn. Cambridge, MA: MIT Press, 2004. 85-100.

Falasiri, Arash, and Nazanin Ghanavizi. "The Persian Blogosphere in Dissent." *Social Media in Iran: Politics and Society after 2009*, Ed. David M. Faris and Babak Rahimi. Albany: State University of New York Press, 2015. 123-36.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32.Stuxnet Dossier." *Symantec*. Feb. 2011. Web. 05 June 2017. <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.

Faris, David M., and Babak Rahimi, eds. *Social Media in Iran: Politics and Society after 2009*. Albany: NY: State University of New York, 2015.

FBI. "Iranians Charged with Hacking U.S. Financial Sector." *Federal Bureau of Investigation (FBI)*. 24 Mar. 2016. Web. 05 June 2017. <https://www.fbi.gov/news/stories/iranians-charged-with-hacking-us-financial-sector>.

Feenberg, Andrew, and Maria Bakardjieva. "Consumers or Citizens? The Online Community Debate." *Community in the Digital Age: Philosophy and Practice*, Ed. Andrew Feenberg and Darin Barney. Lanham, MD: Rowman & Littlefield, 2004. 1-30.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Trans. Alan Sheridan. New York, NY: Vintage, 1977.

——. *The Archaeology of Knowledge*. Trans. A. M. Sheridan Smith. London: Tavistock Publishers, 1972.

Frederick, Howard H. *Global Communication & International Relations*. Belmont, CA: Wadsworth, 1993.

Garrett, R. Kelly. "Protest in an Information Society: A Review of Literature on Social Movements and New ICTs." *Information, Communication & Society* 9.2 (2006): 202-24.

Geers, Kenneth. *Strategic Cyber Security*. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence Publication, 2011.

Gerbaudo, Paolo. *Tweets and the Streets: Social Media and Contemporary Activism*. London: Pluto Press, 2012.

Giacomello, Giampiero. "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism." *Studies in Conflict & Terrorism* 27.5 (2004): 387-408.

Gibson, William. *Neuromancer*. New York City, NY: Ace Books, 1984.

GN. "Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach."*Government of the Netherlands*. 13 August. 2012. Web. 05 June 2017. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf>.

GN. "Interim Report: DigiNotar Certificate Authority Breach "Operation Black Tulip"."*Government of the Netherlands*. 05 Sept. 2011. Web. 05 June 2017. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf>.

Google. "An Update on Attempted Man-in-the-middle Attacks." *Google Online Security Blog*. Google, 29 Aug. 2011. Web. 05 June 2017. <https://security.googleblog.com/2011/08/update-on-attempted-man-in-middle.html>.

Gramsci, Antonio. *Selections from the Prison Notebooks of Antonio Gramsci*. Trans. Quintin Hoare and Geoffrey Nowell-Smith. New York, NY: International, 1971.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. New York, NY: Metropolitan Books, 2014.

Guillen, Mauro F., and Sandra Suarez L. "Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-National Internet Use." *Social Forces* 84.2 (2005): 681-708.

Habermas, Jürgen. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Trans. Thomas Burger. Cambridge, MA: MIT Press, 1989.

Hakim, Simon, and Robert M. Clark, eds. *Cyber-physical Security: Protecting Critical Infrastructure at the State and Local Level*. Switzerland: Springer, 2017.

Hallams, Ellen. "Digital Diplomacy: The Internet, the Battle for Ideas & US Foreign Policy." *CEU Political Science Journal* 5.4, 538-74.

Hammond, Allen L. "Digitally Empowered Development." *Foreign Affairs* 80.2 (2001): 96-106.

Han, Rongbin. "Defending the Authoritarian Regime Online: China's "Voluntary Fifty-cent Army"." *Journal of Current Chinese Affairs* 44.2 (2015): 105-34.

Hannas, Wm C., James Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*. New York: Routledge, 2013.

Hanson, Fergus. "Baked In and Wired: EDiplomacy@State." *Brookings*. 25 October 2012. Web. 08 August 2016. <https://www.brookings.edu/wp-content/uploads/2016/06/baked-in-hansonf-5.pdf>.

Hardy, Keiran, and George Williams. "What Is 'Cyberterrorism'? Computer and Internet Technology in Legal Definitions of Terrorism." *Cyberterrorism Understanding, Assessment, and Response*. Ed. Thomas M. Chen, Lee Jarvis, and Stuart Macdonald. New York, NY: Springer, 2014. 1-23.

Harlow, Summer, and Dustin Harp. "Collective Action on the Web: A Cross-cultural Study of Social Networking Sites and Online and Offline Activism in the United States and Latin America." *Information, Communication & Society* 15.2 (2012): 196-216.

Hayden, Craig. "Engaging Technologies: A Comparative Study of U.S. and Venezuelan Strategies of Influence and Public Diplomacy." *International Journal of Communication* 7 (2013): 1-25.

Heim, Michael. *The Metaphysics of Virtual Reality*. New York: Oxford University Press, 1993.

Hejazi, Arash. "'You Don't Deserve to Be Published'." *Logos* 22.1 (2011): 53-62.

Herold, David Kurt., and Peter Marolt, eds. *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*. Abingdon, Oxon: Routledge, 2011.

Hollon, Cory S. "New Domain, New Direction: Toward a Theory on Cyberspace Control and Use." *Defense Technical Information Center (DTIC)*, 01 Apr. 2012. Web. 01 Mar. 2018. <http://www.dtic.mil/docs/citations/AD1022966>.

Howard, Philip N. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford: Oxford University Press, 2010.

Howard, Philip N., and Muzammil M. Hussain. *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. Oxford: Oxford University Press, 2013.

——. "The Role of Digital Media." *Democratization and Authoritarianism in the Arab World*, Ed. Larry Diamond and Marc F. Plattner. Baltimore: Johns Hopkins University Press, 2014. 186-99.

Hubbard, Amanda, and Lee Bygrave A. "Internet Governance Goes Global." *Internet Governance: Infrastructure and Institutions*, Ed. Lee Bygrave A. and Jon Bing. Oxford: Oxford University Press, 2009. 213-35.

Ide, William. "Iranian Hackers Attack VOA Internet Sites." *Voice Of America (VOA)*. 21 Feb. 2011. Web. 05 June 2017. <https://www.voanews.com/a/iranian-hackers-attack-voa-internet-sites-116678844/172741.html>.

ILSA. "The Iran-Libya Sanctions Act (ILSA)." *The U.S. Government Publishing Office (GPO)*. 05 Aug. 1996. Web. 01 Oct. 2017. <https://www.gpo.gov/fdsys/pkg/STATUTE-110/pdf/STATUTE-110-Pg1541.pdf>.

Inkster, Nigel. "Chinese Intelligence in the Cyber Age." *Survival: Global Politics and Strategy* 55.1 (2013): 45-66.

IP. "The Report of the Commission on the Theft of American Intellectual Property." *The IP Commission*. May 2013. Web. 07 August 2016. <http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf>.

ITU. "Collection of the Basic Texts of the International Telecommunication Union Adopted by the Plenipotentiary Conference (Edition 2015)." *The International Telecommunication Union (ITU)*. 2015. Web. 10 Dec. 2016. <https://www.itu.int/dms_pub/itu-s/oth/02/09/S02090000155201PDFE.PDF>.

——. "Comment From the Administration of the Islamic Republic of Iran on Fourth Draft of the Secretary-general's Report For the Fifth World Telecommunication/information and Communication Technology Policy Forum 2013." *The International Telecommunication Union (ITU)*. 2013. Web. 10 Dec. 2016. <www.itu.int/md/dologin_md.asp?id=S13-WTPF13IEG3-C-0005!!MSW-E>.

——. "Declaration of Principles (Building the Information Society: A Global Challenge in the New Millennium)." *International Telecommunication Union (ITU)*. 12 December 2003. Web. 08 August 2016. <https://www.itu.int/net/wsis/docs/geneva/official/dop.html>.

——. "Final Acts of the World Conference on International Telecommunications (WCIT-12)." *The International Telecommunication Union (ITU)*. 2012. Web. 10 Dec. 2016. <https://www.itu.int/pub/S-CONF-WCIT-2012/en>.

——. "Measuring the Information Society 2009: The ICT Development Index." *The International Telecommunication Union (ITU)*. 2009. Web. 01 Mar. 2017. <https://www.itu.int/ITU-D/ict/publications/idi/material/2009/MIS2009_w5.pdf>.

——. "Measuring the Information Society 2010." *The International Telecommunication Union (ITU)*. 2010. Web. 01 Mar. 2017. <https://www.itu.int/ITU-D/ict/publications/idi/material/2010/MIS_2010_without_annex_4-e.pdf>.

——. "Measuring the Information Society 2011." *The International Telecommunication Union (ITU)*. 2011. Web. 01 Mar. 2017. <https://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf>.

——. "Measuring the Information Society 2012." *The International Telecommunication Union (ITU)*. 2012. Web. 01 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf>.

——. "Measuring the Information Society 2013." *The International Telecommunication Union (ITU)*. 2013. Web. 01 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf>.

——. "Measuring the Information Society Report 2014." *The International Telecommunication Union (ITU)*. 2014. Web. 01 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf>.

——. "Measuring the Information Society Report 2015." *The International Telecommunication Union (ITU)*. 2015. Web. 01 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf>.

——. "Measuring the Information Society Report 2016." *The International Telecommunication Union (ITU)*. 2016. Web. 01 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf>.

——. "Signatories of the Final Acts: 89." World Conference on International Telecommunications (WCIT-12). *The International Telecommunication Union (ITU)*, 14 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/osg/wcit-12/highlights/signatories.html>.

——. "Transcript of the Plenary 1, WCIT-12." *The International Telecommunication Union (ITU)*. 03 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec3plenary1.docx>.

——. "Transcript of the Plenary 2, WCIT-12." *The International Telecommunication Union (ITU)*. 04 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec4plenary2.docx>.

——. "Transcript of the Plenary 3, WCIT-12." *The International Telecommunication Union (ITU)*. 04 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec4plenary3.docx>.

——. "Transcript of the Plenary 4, WCIT-12." *The International Telecommunication Union (ITU).* 07 Dec. 2012. Web. 10 Dec. 2016. <https://www.itu.int/en/wcit-12/Documents/dec7plenary4.docx>.

——. "Tunis Agenda for the Information Society." *International Telecommunication Union (ITU)*. 18 November 2005. Web. 08 August 2016. <http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html>.

Jalava, Jukka, and Matti Pohjola. "ICT as a Source of Output and Productivity Growth in Finland." *Telecommunications Policy* 31.8-9 (2007): 463-72.

JCS. "DOD Dictionary of Military and Associated Terms." *Joint Chiefs of Staff*. Mar. 2018. Web. 01 Apr. 2018. <http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-03-27-153248-110>.

Johnson, Bobbie. "Twitter 'hijacked by Iranian Hackers'." *The Guardian*. 18 Dec. 2009. Web. 05 June 2017. <https://www.theguardian.com/technology/2009/dec/18/twitter-hijacked>.

Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. New York: Routledge, 2000.

——. *Cyberpower: An Introduction to the Politics of Cyberspace*. London: Taylor and Francis, 2002.

Jorgenson, Dale W. "Information Technology and the G7 Economies." *World Economics* 4.4 (2003): 139-69.

——. "Information Technology and the US Economy." *The American Economic Review* 91.1 (March 2001): 1-32.

Jorgenson, Dale, and Kazuyuki Motohashi. "Information Technology and the Japanese Economy." *Journal of the Japanese and International Economies* 19.4 (2005): 460-81.

Kamali Dehghan, Saeed. "Iran Accused of Torturing Blogger to Death." *The Guardian*. 08 Nov. 2012. Web. 05 June 2017. <https://www.theguardian.com/world/2012/nov/08/iran-accused-torturing-blogger-death>.

——. "Iranian Web Programmer Faces Execution on Porn Charges." *The Guardian*. 09 Feb. 2011. Web. 05 June 2017. <https://www.theguardian.com/world/2011/feb/09/iranian-death-sentence-pornography>.

Karimi, Arash. "Rouhani Government Criticizes IRGC Arrests of Journalists." *Al-Monitor*. 06 Apr. 2017. Web. 05 June 2017. <http://www.al-monitor.com/pulse/originals/2017/04/iran-elections-telegram-journalists-channels-arrested.html>.

Karpf, David. *The MoveOn Effect: The Unexpected Transformation of American Political Advocacy*. New York: Oxford University Press, 2012.

——. "Online Political Mobilization from the Advocacy Group's Perspective: Looking Beyond Clicktivism." *Policy & Internet* 2.4 (2010): 7-41.

Kelly, John, and Bruce Etling. "Mapping Iran's Online Public: Politics and Culture in the Persian Blogosphere." *The Berkman Klein Center for Internet & Society at Harvard University*. April 2008. Web. 07 Apr. 2018. <https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/Kelly&Etling_Mapping_Irans_Online_Public_2008.pdf>.

Kelly, Sanja, Mai Truong, Adrian Shahbaz, and Madeline Earp. "Freedom on the Net 2016." *Freedom House*. Nov. 2016. Web. 02 June 2017. <https://freedomhouse.org/sites/default/files/FOTN_2016_BOOKLET_FINAL.pdf>.

Kelly, Sanja, Sarah Cook, and Mai Truong. "Freedom on the Net 2012: A Global Assessment of Internet and Digital Media." *Freedom House*. 24 Sept. 2012. Web. 01 Oct. 2017. <https://freedomhouse.org/sites/default/files/resources/FOTN%202012%20-%20Full%20Report_0.pdf>.

Keohane, Robert O., and Joseph S. Nye. "Power and Interdependence in the Information Age." *Foreign Affairs* 77.5 (1998): 81-94.

——. *Power and Interdependence: World Politics in Transition*. Boston: Little Brown, 1977.

——. "Transgovernmental Relations and International Organizations." *World Politics* 27.01 (1974): 39-62.

Khatami, Mohammad. "Statement by H. E. Mr. Mohammad Khatami President of the Islamic Republic of Iran before the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 10 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/geneva/coverage/archive.asp?lang=en&c_type=pl%7C&c_num=1>.

Khatib, Lina, William Dutton, and Michael Thelwall. "Public Diplomacy 2.0: A Case Study of the US Digital Outreach Team." *The Middle East Journal* 66.3 (2012): 453-72.

Kiggins, Ryan David. "US Leadership in Cyberspace: Transnational Cyber Security and Global Governance." *Cyberspace and International Relations: Theory, Prospects and Challenges*, Ed. Jan-Frederik Kremer and Benedikt Müller. Berlin: Springer, 2014. 161-80.

King, Gary, Robert O. Keohane, and Sidney Verba. *Designing Social Inquiry Scientific Inference in Qualitative Research*. Princeton, NJ: Princeton University Press, 1994.

Kingsley, Patrick. "Inside the Anti-kettling HQ." *The Guardian*. 02 February 2011. Web. 02 August 2016. <https://www.theguardian.com/uk/2011/feb/02/inside-anti-kettling-hq>.

Kitchin, Rob. *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. London: Sage, 2014.

Kozlowski, Andrzej. "Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan." *European Scientific Journal* 3.Special Edition (2014): 237-45.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. *Cyberpower and National Security*. Washington, D.C: Center for Technology and National Security Policy, 2009.

Kronenburg, Ruth, and Farid Haerinejad. "Radio Zamaneh Hacked by Iranian Cyber Army."*Radio Zamaneh*. 01 Feb. 2010. Web. 05 June 2017. <http://www.zamaaneh.com/enzam/2010/02/radio-zamaneh-hacked-by-i.html>.

Kudaisya, Gyanesh. "India's New Mantra: The Internet." *Current History* 100.645 (2001): 162-69.

Kurbalija, Jovan. "Diplomacy in the Age of Information Technology." *Innovation in Diplomatic Practice*, Ed. Jan Melissen. New York: St. Martin's Press, 1999. 171-91

——. "The Impact of the Internet and ICT on Contemporary Diplomacy." *Diplomacy in a Globalizing World: Theories and Practices*, Ed. Pauline Kerr and Geoffrey Wiseman. New York: Oxford University Press, USA, 2013. 141-59.

Kurzman, Charles. "Cultural Jiu-Jitsu and the Iranian Greens." *The People Reloaded: The Green Movement and the Struggle for Iran's Future*. Ed. Nader Hashemi and Danny Postel. Brooklyn, NY: Melville House, 2010. 7-17.

Laer, Jeroen Van, and Peter Van Aelst. "Internet And Social Movement Action Repertoires." *Information, Communication & Society* 13.8 (2010): 1146-171.

Lai, Bruce, and Gale Brewer A. "New York City's Broadband Problem and the Role of Municipal Government in Promoting a Private-sector Solution." *Technology in Society* 28.1-2 (2006): 245-59.

Levinson, Nanette S., and Laura DeNardis. "Governance by Infrustructure." *The Turn to Infrastructure in Internet Governance.* Ed. Francesca Musiani, Derrick L. Cogburn, Laura DeNardis, and Nanette S. Levinson. New York: Palgrave Macmillan, 2016. 3-21.

Lin, Nan. *Social Capital: A Theory of Social Structure and Action*. Cambridge, UK: Cambridge University Press, 2001.

Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22.3 (2013): 365-404.

Lindsay, Jon R., Tai Ming Cheung, and Derek S. Reveron, eds. *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford: Oxford University Press, 2015.

Lipschutz, Ronnie D. "Reconstructing World Politics: The Emergence of Global Civil Society."*Millennium: Journal of International Studies* 21.3 (1992): 389-420.

Lynch, Marc. "The Dialogue of Civilisations and International Public Spheres." *Millennium: Journal of International Studies* 29.2 (2000): 307-30.

Lynn III, William J. "Defending a New Domain." *Foreign Affairs* 89.5 (2010): 97-108.

Machiavelli, Niccolò. "The Prince." *Princeton Readings in Political Thought: Essential Texts since Plato*. Ed. Mitchell Cohen and Nicole Fermon. Princeton, NJ: Princeton University Press, 1996. 167-87.

Malone, Gifford D. "Managing Public Diplomacy." *The Washington Quarterly* 8.3 (1985): 199-213.

Maloney, Suzanne. "Iran: Public Diplomacy in Vacuum." *Isolate or Engage: Adversarial States, US Foreign Policy, and Public Diplomacy*, Ed. Geoffrey Wiseman. Palo Alto: Stanford University Press, 2015. 164-204.

Margetts, Helen. *Information Technology in Government: Britain and America*. London: Routledge, 1999.

Martínez, Diego, Jesús Rodríguez, and José L. Torres. "The Productivity Paradox and the New Economy: The Spanish Case." *Journal of Macroeconomics* 30.4 (2008): 1569-586.

Masoudi Nejad, Reza. "Trans-spatial Public Action The Geography of Iranian Post-Election Protests in the Age of Web 2.0." *Social Media in Iran: Politics and Society after 2009*, Ed. David M. Faris and Babak Rahimi. Albany: State University of New York Press, 2015. 165-82.

Mathiason, John. "The ICANN Experiment." *Internet Governance: The New Frontier of Global Institutions.* London: Routledge, 2009. 70-96.

Mathur, Akshay, and Dhirubhai Ambani. "ICT and Rural Societies: Opportunities for Growth." *The International Information & Library Review* 37.4 (2005): 345-51.

Matsubara, Mihoko. "A Stuxnet Future? Yes, Offensive Cyber-Warfare Is Already Here."*Center for Security Studies*. ETH Zürich, 23 Oct. 2013. Web. 20 Oct. 2017. <http://www.css.ethz.ch/en/services/digital-library/articles/article.html/154091/pdf>.

Mcgraw, Gary. "Cyber War Is Inevitable (Unless We Build Security In)." *Journal of Strategic Studies* 36.1 (2013): 109-19.

McPhail, Clark, and John D. McCarthy. "Protest Mobilization, Protest Repression and Their Interaction." *Repression and Mobilization*, Ed. Christian Davenport, Hank Johnston, and Carol Mueller. Minneapolis: University of Minnesota Press, 2005. 3-32.

Melissen, Jan. "The New Public Diplomacy: Between Theory and Practice." In *The New Public Diplomacy: Soft Power in International Relations*, by Jan Melissen, 3-26. Basingstoke: Palgrave Macmillan, 2005.

Meulen, Nicole Van Der. "DigiNotar: Dissecting the First Dutch Digital Disaster." *Journal of Strategic Security* 6.2 (2013): 46-58.

Michaelsen, Marcus. "The Politics of Online Journalism in Iran." *Social Media in Iran: Politics and Society after 2009*. Ed. David M. Faris and Babak Rahimi. Albany, NY: State U of New York, 2015. 101-22.

MISI. "Measuring the Information Society of Iran (Islamic Rep.) 2015: ICT and Sustainable Development." *The Official Portal of Measuring Information Society of Iran*. Ministry of Information and Communications Technology of Iran, May 2015. Web. 01 Mar. 2017. <http://mis.ito.gov.ir/documents/20182/34805/MIS_IRAN_2015_EN__940320_pub1-edited940323-1.pdf/6e2d53aa-ca0b-4d2d-91fd-d88340663786>.

Morgenthau, Hans J. *Politics among Nations; the Struggle for Power and Peace.* New York: Knopf, 1985.

Morozov, Evgeny. "Foreign Policy: Brave New World Of Slacktivism." *NPR*. 19 May 2009. Web. 01 August 2016. <http://www.npr.org/templates/story/story.php?storyId=104302141>.

——. *The Net Delusion the Dark Side of Internet Freedom*. New York, NY: PublicAffairs, 2011.

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.

Murray, Stuart. "Evolution, Not Revolution: The Digital Divide in American and Australian Contexts." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 127-44.

Nah, Seungahn, Aaron S. Veenstra, and Dhavan V. Shah. "The Internet and Anti-War Activism: A Case Study of Information, Expression, and Action." *Journal of Computer-Mediated Communication* 12.1 (2006): 230-47.

Nakashima, Ellen. "Cyberattack on Mideast Energy Firms Was Biggest Yet, Panetta Says."*The Washington Post*. 11 Oct. 2012. Web. 05 June 2017. <https://www.washingtonpost.com/world/national-security/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html?>.

Nakashima, Ellen, and Joby Warrick. "Stuxnet Was Work of U.S. and Israeli Experts, Officials Say." *The Washington Post*. 02 June 2012. Web. 05 June 2017. <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.0f7912d38fe6>.

Nakashima, Ellen, Greg Miller, and Julie Tate. "U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say." *The Washington Post*. 19 June 2012. Web. 05 June 2017. <https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.e2052df3ea63>.

Natarajan, Kalathmika. "Digital Public Diplomacy and a Strategic Narrative for India." *Strategic Analysis* 38.1 (2014): 91-106.

Nielsen, Rasmus Kleis. "The Labors of Internet-Assisted Activism: Overcommunication, Miscommunication, and Communicative Overload." *Journal of Information Technology & Politics* 6.3-4 (2009): 267-80.

NM. "Contribution from the Islamic Republic of Iran to The Global Multistakeholder Meeting for the Future of the Internet, 23-24 April 2014 Sao Paolo, Brazil." *NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance*. 2014. Web. 10 Dec. 2016. <http://content.netmundial.br/files/236.pdf>.

——. "NETmundial Multistakeholder Statement." *NETmundial – Global Multistakeholder Meeting on the Future of Internet Governance*., 24 Apr. 2014. Web. 10 Dec. 2016. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>.

Noble, David. "Computers Will Create Unemployment." *Computers and Society*. Ed. Paul A. Winters. San Diego, CA: Greenhaven, 1997. 40-43.

Norris, Pippa. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. New York: Cambridge University Press, 2001.

NTIA. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." *National Telecommunications and Information Administration.* United States Department of Commerce, 14 Mar. 2014. Web. 10 Dec. 2016. <https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

Nye, Joseph S. "How Sharp Power Threatens Soft Power." *Foreign Affairs*. 24 Jan. 2018. Web. 07 Apr. 2018. <http://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power>.

——. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Winter 2011, 20-38.

Nye, Joseph S. *Bound to Lead: The Changing Nature of American Power*. New York: Basic, 1990.

——. *Cyber Power*. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.

——. *The Future of Power*. New York, NY: PublicAffairs, 2011.

——. *The Paradox of American Power: Why the World's Only Superpower Can't Go It Alone*. Oxford: Oxford University Press, 2003.

——. *Power in the Global Information Age: From Realism to Globalization*. New York, NY: Routledge, 2004.

——. *Soft Power the Means to Success in World Politics*. New York: PublicAffairs, 2004.

NYT. "Hacking in the Netherlands Took Aim at Internet Giants." *The New York Times*. 05 Sept. 2011. Web. 05 June 2017. <http://www.nytimes.com/2011/09/06/technology/hacking-in-the-netherlands-broadens-in-scope.html>.

ONCE. "Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011." *Office of the National Counterintelligence Executive*. October 2011. Web. 07 August 2016. <https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf>.

Oulton, Nicholas. "ICT and Productivity Growth in the United Kingdom." *Oxford Review of Economic Policy* 18.3 (2002): 363-79.

Ozbilgin, Ozge. *Turkey Tightens Internet Controls, Weeks into New Government*. Sept. 2014. Web. 02 Jan. 2015. <https://www.reuters.com/article/us-turkey-internet/turkey-tightens-internet-controls-weeks-into-new-government-idUSKBN0H419T20140909>.

Park, Se Jung, and Yon Lim Soo. "Information Networks and Social Media Use in Public Diplomacy: A Comparative Analysis of South Korea and Japan." *Asian Journal of Communication* 24.1 (2014): 79-98.

Pastebin. "Untitled." *Pastebin*. 15 Aug. 2012. Web. 05 June 2017. <https://pastebin.com/HqAgaQRj>.

Paxton, Pamela. "Social Capital and Democracy: An Interdependent Relationship." *American Sociological Review* 67.2 (2002): 254-77.

Pelling, Jon. "When Doing Becomes the Message: The Case of the Swedish Digital Diplomacy." *Digital Diplomacy: Theory and Practice*, Ed. Corneliu Bjola and Marcus Holmes. New York: Routledge, 2015. 164-80.

Pesaran, Evaleila. "Resurrecting the Revolution." *Iran's Struggle for Economic Independence: Reform and Counter-reform in the Post-revolutionary Era*. London: Routledge, 2013. 128-60.

Pfeifle, Mark. "A Nobel Peace Prize for Twitter?" *The Christian Science Monitor*. 06 July 2009. Web. 01 Oct. 2017. <http://www.csmonitor.com/Commentary/Opinion/2009/0706/p09s02-coop.html>.

Pool, Ithiel de Sola. *Technologies of Freedom*. Cambridge, MA: Harvard University Press, 1983.

Press TV. "'Iran Set to Build First Cyber Army'." *Press TV*. 20 Feb. 2012. Web. 05 May 2017. <https://web.archive.org/web/20120621015437/http://www.presstv.ir/detail/227739.html>.

Putnam, Robert D. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000.

Rahimi, Babak. "The Politics of the Internet in Iran." *Media, Culture and Society in Iran: Living with Globalization and the Islamic State*, Ed. Mehdi Semati. London: Routledge, 2008. 37-56.

Ramazani, R. K. "The Shifting Premise of Iran's Foreign Policy: Towards a Democratic Peace?" *Middle East Journal* 52.2 (1998): 177-87.

Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." *Explorations in Cyber International Relations*, 1 Apr. 2012, <https://goo.gl/F1kuaK>.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35.1 (2012): 5-32.

Rininsland, Ændrew. "Internet Censorship Listed: How Does Each Country Compare?" *The Guardian*. 16 April 2012. Web. 06 August 2016. <https://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list>.

Ronfeldt, David, and Danielle Varda. "The Prospects for Cyberocracy (Revisited)." *Social Science Research Network (SSRN)*. 01 Dec. 2008. Web. 01 August 2016. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1325809>.

Rosecrance, Richard N. *The Rise of the Virtual State: Wealth and Power in the Coming Century*. New York, NY: Basic, 1999.

Rosenau, James N. *Along the Domestic-Foreign Frontier: Exploring Governance in a Turbulent World.* New York, NY: Cambridge University Press, 1997.

Saadoun, Mélissa, and Lin Yanning. "Research, Innovation and Technological Development." *Innovation Engineering: the Power of Intangible Networks*. Ed. Patrick Corsi et al. Newport Beach, CA: ISTE, 2006. 85-104.

Sabet-Saeidi, Shahriar. "Iranian–European Relations: A Strategic Partnership?" *Iran's Foreign Policy: From Khatami to Ahmadinejad*. Ed. Anoushirvan Ehteshami and Mahjoob Zweiri. Berkshire: Ithaca, 2012. 55-72.

Sabety, Setareh. "Graphic Content: The Semiotics of a YouTube Uprising." *Media, Power, and Politics in the Digital Age: The 2009 Presidential Election Uprising in Iran*, Ed. Yahya R. Kamalipour. Lanham, MD: Rowman & Littlefield Publishers, 2010. 119-24.

Sadeghi Esfahani, Mohammad. "The Politics and Anti-Politics of Facebook in Context of the Iranian 2009 Presidential Elections and Beyond." *Social Media in Iran: Politics and Society after 2009*. Ed. David M. Faris and Babak Rahimi. Albany, NY: State University of New York, 2016. 137-64.

Safshekan, Roozbeh. "Iran and the Global Politics of Internet Governance." *Journal of Cyber Policy* 2.2 (2017): 266-84.

——. "The Matrix of Communication in Social Movements: A Comparison of the 1979 Revolution and 2009 Green Movement in Iran." *Sociology of Islam* 2.3-4 (2014): 328-45.

Salhi, Hamoud. "Assessing Theories of Information Technology and Security for the Middle East." *International Relations and Security in the Digital Age*. Ed. Johan Eriksson and Giampiero Giacomello. London: Routledge, 2007. 106-31.

Schmidt, Eric, and Jared Cohen. *The New Digital Age: Transforming Nations, Businesses, and Our Lives*. New York, NY: Knopf Doubleday Publishing Group, 2013.

Schmitt, Michael N., ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge: Cambridge University Press, 2013.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016, 115.

Seib, Philip M. *Real-time Diplomacy: Politics and Power in the Social Media Era*. New York: Palgrave Macmillan, 2012.

Shah, Dhavan V., Jaeho Cho, William P. Eveland JR., and Nojin Kwak. "Information and Expression in a Digital Age: Modeling Internet Effects on Civic Participation." *Communication Research* 32.5 (2005): 531-65.

Shaheen, Salma. "Offense–Defense Balance in Cyber Warfare." *Cyberspace and International Relations Theory, Prospects and Challenges*. Ed. Jan-Frederik Kremer and Benedikt Müller. Berlin: Springer Berlin, 2016. 77-94.

Shahidi, Hossein. "From Mission to Profession: Journalism in Iran, 1979-2004." *Iranian Studies* 39.1 (2006): 1-28.

——. *Journalism in Iran from Mission to Profession*. London: Routledge, 2010.

Sheldon, John B. "The Rise of Cyberpower." *Strategy in the Contemporary World*, Ed. John Baylis, James J. Wirtz, and Colin S. Gray. 4th ed. Oxford: Oxford University Press, 2009. 303-19.

Signitzer, Benno H., and Timothy Coombs. "Public Relations and Public Diplomacy: Conceptual Convergences." *Public Relations Review* 18.2 (1992): 137-47.

Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press, 2014, 140.

SM. "Internet Infrastructure and Policy Report - March 2014." *Small Media*. Mar. 2014. Web. 01 June 2017. <https://www.smallmedia.org.uk/old/content/114.html>.

Sreberny, Annabelle, and Gholam Khiabany. Blogistan: *The Internet and Politics in Iran*. London: I.B. Tauris, 2010.

Starr, Stuart H. "Towards an Evolving Theory of Cyberpower." *The Virtual Battlefield: Perspectives on Cyber Warfare*. Ed. Christian Czosseck and Kenneth Geers. Washington, DC: IOS, 2009. 18-52.

Stein, Jeff. "The Latest Document From the Snowden Trove Highlights Israeli Spying." *Newsweek*.16 May 2014. Web. 07 Apr. 2018. <http://www.newsweek.com/mostly-good-week-israel-us-spying-controversy-251261>.

Stone, John. "Cyber War Will Take Place!" *Journal of Strategic Studies* 36.1 (2013): 101-08.

Symantec. "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East." *Symantec*. 28 May 2012. Web. 05 June 2017. <https://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east>.

——. "W32.Duqu: The Precursor to the next Stuxnet." *Symantec*. 23 Nov. 2011. Web. 05 June 2017. <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>.

Tabansky, Lior, and Isaac Ben-Israel. *Cybersecurity in Israel*. London: Springer, 2015.

Tahmasebi, Sussan. "Iranian Civil Society Organizations Training and Research Center." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 17 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/tunis/scripts/archive.asp?lang=en&c_type=2|17&c_num=301>.

Tai, Zixue. *The Internet in China: Cyberspace and Civil Society*. New York: Routledge, 2006.

Thucydides. *History of the Peloponnesian War*. Trans. Richard Crawley. Mineola, NY: Dover Publication, 2017.

Tibet Action Institute. "Tibet: Frontline of the New Cyberwar." *YouTube*, 27 Jan. 2015. Web. 07 Apr. 2018. <http://www.youtube.com/watch?v=yE3AQqbGVkk.%2BAccessed%2B1%2BFeb.%2B2015.>.

Tilly, Charles. *From Mobilization to Revolution*. MA: Addison-Wesley Publishing Company, 1978.

——. "Repertoires of Contention in America and Britain, 1750-1830." *The Dynamics of Social Movements: Resource Mobilization, Social Control, and Tactics*, Ed. Mayer N. Zald and John D. McCarthy. Cambridge, MA: Winthrop Publishers, 1979. 126-55.

UN. "32/13. The Promotion, Protection and Enjoyment of Human Rights on the Internet." *The United Nations*. 18 July 2014. Web. 10 Dec. 2016. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf>.

——. "68/302. Modalities for the Overall Review by the General Assembly of the Implementation of the Outcomes of the World Summit on the Information Society." *The United Nations*. 13 Aug. 2014. Web. 10 Dec. 2016. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/302>.

——. "70/1. Transforming Our World: The 2030 Agenda for Sustainable Development." *The United Nations*. 21 Oct. 2015. Web. 10 Dec. 2016. <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E>.

——. "70/125. Outcome Document of the High-level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society." *The United Nations*. 01 Feb. 2016. Web. 10 Dec. 2016. <http://unctad.org/en/PublicationsLibrary/ares70d125_en.pdf>.

——. "Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General." *The United Nations*. 09 Sept. 2013. Web. 10 Dec. 2016. <http://www.un.org/ga/search/view_doc.asp?symbol=A/68/156/Add.1>.

——. "UN E-Government Survey 2003." *The United Nations*. 2003. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2003>.

——. "UN E-Government Survey 2004." *The United Nations*. 2004. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2004>.

——. "UN E-Government Survey 2005." *The United Nations*. 2005. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2005>.

——. "UN E-Government Survey 2008." *The United Nations*. 2008. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2008>.

——. "UN E-Government Survey 2010." *The United Nations*. 2010. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010>.

——. "UN E-Government Survey 2012." *The United Nations*. 2012. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2012>.

——. "UN E-Government Survey 2014." *The United Nations*. 2014. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014>.

——. "UN E-Government Survey 2016." *The United Nations*. 2016. Web. 01 Mar. 2017. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016>.

UNCTD. "The Digital Divide: ICT Development Indices 2004." *United Nations Conference on Trade and Development*, 2004. Web. 10 Dec. 2016. <http://unctad.org/en/docs/iteipc20054_en.pdf>.

UNESCO. "Education 2030: Incheon Declaration and Framework for Action for the Implementation of Sustainable Development Goal 4." *The United Nations Educational, Scientific and Cultural Organization*, 2016, unesdoc.unesco.org/images/0024/002456/245656E.pdf.

UNIDR. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Institute for Disarmament Research*. The United Nations, 24 June 2013. Web. 10 Dec. 2016. <http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-578.pdf>.

UNPAN. "Statement by Delegation of the Islamic Republic of Iran 2nd Second Preparatory Meeting for the General Assembly's Overall Review of the Implementation of the Outcomes of the WSIS." *United Nations Public Administration Network*. The United Nations, 22 Oct. 2015. Web. 10 Dec. 2016. <http://workspace.unpan.org/sites/Internet/Documents/UNPAN95484.pdf>.

USDS. "21st Century Statecraft." *U.S. Department of State*. 2009. Web. 11 August 2016. <http://www.state.gov/statecraft/overview/index.htm>.

Van Aelst, Peter, and Stefaan Walgrave. "New Media, New Movements? The Role of the Internet in Shaping the 'anti-globalization' Movement." *Cyberprotest: New Media, Citizens and Social Movements*. Ed. Wim Van De Donk, Brian D. Loader, Paul G. Nixon, and Dieter Rucht. London: Routledge, 2004. 87-108

Van Djik, Jan A. G. M. "One Europe, Digitally Devide." *Routledge Handbook of Internet Politics*, Ed. Andrew Chadwick and Philip N. Howard, 288-304. London: Routledge, 2009. 288-304.

Van Laer, Jeroen. "Activists "online" and "offline": Internet as an Information Channel for Protest Demonstrations." *Mobilization: An International Journal* 15.3 (2010): 405-21.

Van Noort, Carolijn. *Social Media Strategy: Bringing Public Diplomacy 2.0 to the next Level*. San Francisco: Consulate General of the Netherlands, 2011.

Vasi, Ion Bogdan, and Chan S. Suh. "Online Activities, Spatial Proximity, and the Diffusion of the Occupy Wall Street Movement in the United States." *Mobilization: An International Quarterly* 21.2 (2016): 139-54.

VEUS. "Why Virtual Embassy?" *Virtual Embassy of the United States - Tehran, Iran*. Web. 07 Apr. 2018. <https://ir.usembassy.gov/tehran/>.

Vu, Khuong M. "ICT as a Source of Economic Growth in the Information Age: Empirical Evidence from the 1996–2005 Period." *Telecommunications Policy* 35.4 (2011): 357-72.

——. "Information and Communication Technology (ICT) and Singapore's Economic Growth." *Information Economics and Policy* 25.4 (2013): 284-300.

Walker, Christopher, and Jessica Ludwig. "The Meaning of Sharp Power." *Foreign Affairs*, 16 Nov. 2017. Web. 07 Apr. 2018. <https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power>.

Wallimann, Isidor, Nicholas Ch. Tatsis, and George V. Zito. "On Max Weber's Definition of Power." *Journal of Sociology* 13.1 (1977): 231-35.

Waltz, Kenneth Neal. *Theory of International Politics*. Reading, MA: Addison-Wesley, 1979.

WB. "Information and Communications for Development: Global Trends and Policies." *The World Bank*. 2006. Web. 08 August 2016. <http://documents.worldbank.org/curated/en/692321468170348192/Overview>.

——. "World Development Report 2016: Digital Dividends." *The World Bank*. 2016. Web. 07 August 2016. <http://www.worldbank.org/en/publication/wdr2016>.

Weber, Max. "Politics as a Vocation." *From Max Weber: Essays in Sociology*. Ed. Hans Gerth and C. Wright Mills. Abingdon, Oxon: Routledge, 1991. 77-128.

——. *The Theory of Social and Economic Organization*. New York, NY: Oxford University Press, 1947.

WEF. "The Global Information Technology Report 2010–2011: Transformations 2.0." *The World Economic Forum*. 2011. Web. 01 Mar. 2017. <http://reports.weforum.org/global-information-technology-2011/>.

——. "The Global Information Technology Report 2012: Living in a Hyperconnected World." *The World Economic Forum*. 2012. Web. 01 Mar. 2017. <http://reports.weforum.org/global-information-technology-2012/>.

——. "The Global Information Technology Report 2013: Growth and Jobs in a Hyperconnected World." *The World Economic Forum*. 2013. Web. 01 Mar. 2017. <http://reports.weforum.org/global-information-technology-report-2013/>.

——. "The Global Information Technology Report 2014: Rewards and Risks of Big Data." *The World Economic Forum*. 2014. Web. 01 Mar. 2017. <http://reports.weforum.org/global-information-technology-report-2014/>.

——. "The Global Information Technology Report 2015: ICTs for Inclusive Growth." *The World Economic Forum*. 2015. Web. 01 Mar. 2017. <https://reports.weforum.org/global-information-technology-report-2015/>.

——. "The Global Information Technology Report 2016: Innovating in the Digital Economy." *The World Economic Forum*. 2016. Web. 01 Mar. 2017. <https://www.weforum.org/reports/the-global-information-technology-report-2016>.

Weimann, Gabriel. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3.2 (2012): 75-90.

——. *Terrorism in Cyberspace: The next Generation*. New York: Columbia University Press, 2015.

Wendt, Alexander. *Social Theory of International Politics*. Cambridge: Cambridge University Press, 1999.

Williams, Dmitri. "On and Off the 'Net: Scales for Social Capital in an Online Era." *Journal of Computer-Mediated Communication* 11.2 (2006): 593-628.

WSIS. "Brazilian Government Contribution (WSIS/PC-3/CONTR/60-E)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 31 May 2003. Web. 10 Dec. 2016. <https://www.itu.int/dms_pub/itu-s/md/03/.../S03-WSISPC3-C-0060!!MSW-E.doc>.

——. "Geneva Declaration of Principles (WSIS-03/GENEVA/DOC/0004)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 12 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161|1160>.

——. "I PrepCom for the World Summit on Information Society: Statement from Brazil." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 5 July 2002. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing-all-pc.asp?lang=en&c_event=pc|1>.

——. "Islamic Republic of Iran (WSIS/PC-3/C/0084)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 31 May 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing-all-pc.asp?lang=en&c_event=pc|3>.

——. "Participation." *World Summit on the Information Society*. The International Telecommunication Union (ITU), Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/participation/index.html>.

——. "Proposal on Internet Governance Islamic Republic of Iran (WSIS-II/PC-3/DT/22)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 30 Sept. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing.asp?lang=en&c_event=pc2%7C3&c_type=td%7C>.

——. "Shaping Information Societies for Human Needs: Civil Society Declaration to the World Summit on the Information Society." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 8 Dec. 2003. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en?&id=1179|1208>.

——. "Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6 (rev. 1))." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 18 Nov. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=2266|2267>.

——. "Tunis Phase: Civil Society Declaration (WSIS-05/TUNIS/CONTR/13)." *World Summit on the Information Society*. The International Telecommunication Union (ITU), 23 Dec. 2005. Web. 10 Dec. 2016. <https://www.itu.int/net/wsis/documents/listing-all.asp?lang=en&c_event=s|2&c_type=all|>.

Yahyanejad, Mehdi. "The Effectiveness of Internet for Informing and Mobilizing in the Events after the Iranian Presidential Election." *Massachusetts Institute of Technology (MIT).* 2010. Web. 07 Apr. 2018. <groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2010/weeks/week12-Yahyenejad.pdf>.

Yahyanedjad, Mehdi, and Elham Gheytanchi. "Social Media, Dissent, and Iran's Green Movement." *Liberation Technology: Social Media and the Struggle for Democracy*. Ed. Larry Diamond and Marc F. Plattner. Baltimor, Md: John Hopkins University Press, 2012. 139-53.

Yang, Guobin. *The Power of the Internet in China: Citizen Activism Online*. New York: Columbia University Press, 2009.

Zetter, Kim. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown Publishers, 2014.

Zhong, Xin, and Jiayi Lu. "Public Diplomacy Meets Social Media: A Study of the U.S. Embassy's Blogs and Micro-blogs." *Public Relations Review* 39.5 (2013): 542-48.

Zittrain, Jonathan, and Rafal Rohozinski. "Internet Filtering: The Politics and Mechanisms of Control." *Access Denied: The Practice and Policy of Global Internet Filtering*, Ed. Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: MIT Press, 2008. 29-56.

Zixue, Tai. "The Great Firewall." *The Internet in China: Cultural, Political, and Social Dimensions,1980s-2000s*, Ed. Ashley Esarey and Randy Kluver. Great Barrington: Berkshire Publishing Group, 2014. 64-74.

Persian Sources

BBC. "Hamleh-ye Interneti-ye Tazeh Be Site-haye Interneti-ye Motarezan-e Irani (New Cyber Attack Against the Iranian Protestors' Websites)." *BBC Persian*. The British Broadcasting Corporation (BBC), 12 Feb. 2010. Web. 05 June 2017. <http://www.bbc.com/persian/iran/2010/02/100212_l06_jaras_kalameh_hacking.shtml>.

BTA. "Gharargah-e Jang-e Cyberi Rahandazi Mishavad (The Cyber Warfare Headquarters Will Be Stablished)." *Bultan News Agency*. 06 Mar. 2011. Web. 05 June 2017. <http://www.bultannews.com/fa/news/41662>.

CP. "Sharh-e Vazayef Va Mamuriat-ha (Overview of Missions and Responsibilities)." *The Cyber Police*. Web. 05 June 2017. <http://www.cyberpolice.ir/page/127>.

CPK. "Sanad-e Cheshm Andaz-e Jomhuri-ye Eslami-ye Iran Dar Ofogh-e 1404 (2025 Horizon Vision Document of the Islamic Republic of Iran)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei*. 04 Nov. 2003. Web. 01 Mar. 2017. <http://farsi.khamenei.ir/message-content?id=9034>.

Dey 9th. "Ghoveh-ye Ghazaieh Dar Barkhord Ba Saran-e Fetneh Barkhord-e Amali Konad (The Judiciary Shall Take Concrete Measures to Confront the Sedition Leaders)." *Dey 9th Weekly Newspaper*. 26 Apr. 2011. Web. 05 June 2017. <https://web.archive.org/web/20111101184327/http://www.9day.ir:80/article/274>.

EDCS. "Siasatha-ye Kolli-ye Shabakeh-haye Ettelaresani-ye Rayaneh-i (Comprehensive Policies for Computer Information Networks)." *Expediency Discernment Council of the System*. 03 Oct. 1998. Web. 03 June 2017. <http://81.91.157.27/DocLib2/Approved%20Policies/Offered%20General%20Policies/approved%20general%20policy%20%20%2018-08-1372%20of%20%20ettelaresani.aspx.html>.

FNA. "Goftegu-ye Tafsili-ye Fars Ba Vazir-e Ertebatat Va Fanavari Ettelaat (Fars' Extensive Conversation with the Minister of Communication and Information Technology)." *Fars News Agency*. 23 July 2006. Web. 01 June 2017. <http://www.farsnews.com/8505010040>.

——. "Morurgar-e 'Irani' Copy-e Raigan-e Firefox Az Aab Dar Aamad (The 'Iranian' Browser Appears to Be a Free Replica of Firefox)." *Fars News Agency*. 24 Dec. 2013. Web. 02 June 2017. <http://www.farsnews.com/newstext.php?nn=13921003000651>.

Gerdab. "Farmandehi-ye Amniat-e Cyberi-ye Sepah-e Pasdaran-e Enghelab-e Eslami (The Cyber Security Command of the Islamic Revolutionary Guard Corps)."*Gerdab*. The IRGC Cyber Security Command, Web. 05 June 2017. <http://www.gerdab.ir/fa/about>.

——. "System Aml-e Bumi-ye Ghasedak Eraeh Shod (Indigenous Ghasedak Operating System Is Released)." *Gerdab*. Center for the Investigation of Organized Cybercrimes (CIOC), 28 Aug. 2012. Web. 01 June 2017. <http://www.gerdab.ir/fa/news/12033>.

——. "Tarikhcheh-ye Parvandehha-ye Rasanehi-ye Shodeh-ye Gerdab (The Record of Gerdab's Publicized Files)." *Gerdab*. The IRGC Cyber Security Command, 15 Sept. 2015. Web. 05 June 2017. <http://www.gerdab.ir/fa/news/15588>.

Ghasedak. "Download-e System-e Amel-e Bumi-ye Ghasedak (Indigenous Ghasedak Operating System Download)." *Markaz-e Poshtibani-ye Online Ghasedak (Ghasedak Online Support Center)*, 1 Sept. 2012. Web. 01 June 2017. <http://support.qsdk.com/index.php?_m=downloads&_a=viewdownload&downloaditemid=110&nav=0>.

IPRC. "Ghanun-e Barnameh-ye Panjsaleh-ye Panjom-e Tose-ye Jomhuri-ye Eslami-ye Iran (1390-1394) (Fifth Five Year Plan of the Islamic Republic of Iran (2011-2015))." *Islamic Parliament Research Center of the Islamic Republic of Iran*. 20 Jan. 2011. Web. 01 June 2017. <http://rc.majlis.ir/fa/law/show/790196>.

ISNA. "Ejraye Phase-e Bolughe Shabakeh-ye Melli-ye Ettelaat Ta Payan Dolat (The implementation of the Maturiy Phase of the Nation Information Network by the End of the Administration)." *Iranian Students' News Agency (ISNA)*. 06 Feb. 2017. Web. 02 June 2017. <http://www.isna.ir/news/95111812481/>.

——. "Mahvareh Va Internet Amad Vali Hoviat-e Jvan-e Ma Az Dast Naraft (Satellite and the Internet Came but Our Youth's Identity Was Not Lost)." *Iranian Students' News Agency (ISNA)*. 17 May 2014. Web. 03 June 2017. <http://www.isna.ir/news/93022716896>.

ITDMC. "Sanad-e Rahbori-ye Padafand-e Cyberi-ye Keshvar (The Country's Cyber Defense Strategic Document)." *Information Technology and Digital Media Center*. Ministry of Culture and Islamic Guidance, 11 June 2015. Web. 05 June 2017. <http://www.saramad.ir/Content/media/filepool3/2015/11/2946.pdf>.

IWMH. "Matn-e Kamel-e Ayinnameh-ye Samandehi-ye Paygahha-ye Interneti-ye Irani (The Full Text of the Managing Iranian Internet Websites Statute)." *The Internet Websites Managing Headquarters*. The Ministry of Culture and Islamic Guidance, 20 Aug. 2006. Web. 03 June 2017. <http://95.38.61.77/samHelp/regulation.html>.

Jafari, Mehrdad. "Hameh Ba Ham Baraye Amniat Va Aramesh (All together for Security and Tranquillity)." *The Cyber Police*. Web. 05 June 2017. <http://www.cyberpolice.ir/sites/default/files/fata.pdf>.

Khamenei, Ali. "Bayanat Dar Jam-e Kasiri Az Basijian-e Keshvar (A Speech to a Large Crowd of the Nation's Basij)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei*. 25 Nov. 2009. Web. 26 Oct. 2017. <http://farsi.khamenei.ir/speech-content?id=8430>.

——. "Hokm-e Entesaab Aza-Ye Shora-Ye Aali-Ye Faza-Ye Majazi (The Decree for the Appointment of the Members of the Supreme Council of Cyberspace)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei.* 05 Sep. 2015. Web. 03 June 2017. <http://farsi.khamenei.ir/print-content?id=30658>.

——. "Hokm-e Tashkil Va Entesaab Aza-ye Shora-ye Aali-ye Faza-ye Majazi (The Decree for the Formation and Appointment of the Members of the Supreme Council of Cyberspace)." *The Center for Preserving and Publishing the Works of Grand Ayatollah Sayyid Ali Khamenei.* 07 Mar. 2012. Web. 03 June 2017. <http://farsi.khamenei.ir/print-content?id=19225>.

——. *Instagram*, 01 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTjgNbkBWbc>.

——. *Instagram*, 02 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BU12qUcBPas>.

——. *Instagram*, 06 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVAft5XB9sj>.

——. *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTyR3VwBeRu>.

——. *Instagram*, 10 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BStg3Pqh4I2>.

——. *Instagram*, 15 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVW-lS6hJD5>.

——. *Instagram*, 16 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVZVGGBBuQ_>.

——. *Instagram*, 18 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVfqTf2BKNS>.

——. *Instagram*, 21 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTJ99sLBQUo>.

——. *Telegram*, 07 June 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6215>.

——. *Telegram*, 12 June 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6280>.

——. *Telegram*, 21 June 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6365>.

——. *Telegram*, 24 May 2017. Web. 02 Sept 2017. <https://t.me/khamenei_ir/6054>.

Khatami, Mohammad. *Instagram*, 06 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BU_j1ojAdAQ>.

——. *Instagram*, 10 June 2017. Web. 02 Sept 2017. https://www.instagram.com/p/BVKcVkQgcRC>.

——. *Instagram*, 18 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTCDIdNAo1T/>.

——. *Instagram*, 19 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BURNx7ZAoZh/>.

——. *Telegram*, 11 June 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/529>.

——. *Telegram*, 12 June 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/531>.

——. *Telegram*, 13 June 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/533>.

——. *Telegram*, 14 May 2016. Web. 02 Sept 2017. <https://t.me/khatamimedia/468>.

——. *Telegram*, 21 Feb. 2016. Web. 02 Sept 2017. <https://t.me/khatamimedia/150>.

——. *Telegram*, 29 May 2017. Web. 02 Sept 2017. <https://t.me/khatamimedia/511>.

Khomeini, Ruhollah. "Sahifeh-ye Imam. Vol. 14." *The Institute for Compilation and Publication of Imam Khomeini's Works*. Web. 05 June 2017. <http://statics.ml.imam-khomeini.ir/en/File/NewsAttachment/2014/1708-Sahifeh-ye%20Imam-Vol%2014.pdf>.

LMDCICA. *Library, Museum and Document Center of the Islamic Consultative Assembly*. Web. 02 June 2017. <http://www.ical.ir>.

MISI. "Vaziat-e Tose-ye Fanavari-ye Ettela'at Va Ertebatat Keshvar (The Country's State of Information and Communication Technology Development)." *The Official Portal of Measuring Information Society of Iran*. Ministry of Information and Communications Technology of Iran, 2015. Web. 01 Mar. 2017. <http://mis.ito.gov.ir/documents/20182/34805/ict94/63cb5ef2-982e-4fbc-9c81-120a0a83e765>.

MNA. "Dastur-e Reis-e Jomhur Baraye Tavaghof-e Filter-e 'WhatsApp' (The President's Order to Stop the 'WhatsApp' Ban)." *Mehr News Agency*. 06 May 2014. Web. 03 June 2017. <http://www.mehrnews.com/news/2285832>.

—— "Enfejarha Va Havades-e Akhir Az Tarigh Fazaye Majazi Modiriat Mishavad (Recent Explosions and Incidences are Managed through Cyberspace)." *Mehr News Agency*. 23 Jan. 2011. Web. 05 June 2017. <http://www.mehrnews.com/news/1238040>.

—— "Farman-e Tashkil-e Gharargah-e Cyberi Dar Keshvar Eblagh Shod (The Decree for the Formation of the Cyber Defense Headquarters in the Country Was Issued)." *Mehr News Agency*. 30 Oct. 2011. Web. 05 June 2017. <http://www.mehrnews.com/news/1447810>.

—— "Joziat-e System-e Amel-e Bumi-e Xamin (Details of the Indigenous Xamin Operating System)." *Mehr News Agancy*. 23 June 2012. Web. 01 June 2017. <http://www.mehrnews.com/news/1632002>.

—— "Morurgar-e Saina Jaygozin-e Explorer Va Firefox (Saina Browser as a Substitution for Explorer and Firefox)." *Mehr News Agency*. 01 Oct. 2013. Web. 02 June 2017. <http://www.mehrnews.com/news/2140769>.

—— "Mosahebeh-ye Mehr Ba Vazir-e Ertebatat Va Fanavari Ettelaat (Mehr's Interview with the Minister of Communication and Information Technology)." *Mehr News Agency*. 04 Jan. 2011. Web. 02 June 2017. <http://www.mehrnews.com/news/1224464>.

—— "Nahveh-ye Hemayat Az Motorha-ye Jostejuy-e Boomi (The way the Government supports the indigenous search engines)." *Mehr News Agency*. 08 May 2015. Web. 02 June 2017. <http://www.mehrnews.com/news/2571884>.

—— "Panj Million Website Dar Keshvar Filter Shodeh Ast (Five Million Websites Have Been Filtered in the Country)." *Mehr News Agency*. 18 Nov. 2008. Web. 03 June 2017. <http://www.mehrnews.com/news/784979>.

—— "Rahandazi-e Motor Jostejoogar-e Irani (Initiation of an Iranian Search Engine)."*Mehr News Agency*. 15 Feb. 2015. Web. 02 June 2017. <http://www.mehrnews.com/news/2495783>.

—— "Tashkile Setad-e Bohran-e Cyberi Dar Vezarat-e Naft (Formation of the Cyber Crisis Headquarters in the Oil Ministry)." *Mehr News Agency*. 23 Apr. 2012. Web. 05 June 2017. <http://www.mehrnews.com/news/1584142>.

Motahari, Ali. *Instagram*, 13 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUC8XsZhk-Q>.

——. *Instagram*, 23 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUcQDi_hFNR>.

——. *Telegram*, 01 June 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/605>.

——. *Telegram*, 13 May 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/583>.

——. *Telegram*, 22 May 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/595>.

——. *Telegram*, 27 June 2017. Web. 02 Sept 2017. <https://t.me/alimotahari_ir/623>.

MPO. "Layeh-ye Budge-ye Sal-e 1396 Kol-e Keshvar (The Country's 2017 Budget Bill)." *Management and Planning Organization of Iran*. 2016. Web. 02 June 2017. <http://www.mporg.ir/FileSystem/View/File.aspx?FileId=698c98e6-743d-49ad-8885-d23ccf2d1448>.

NCC. "Shabakeh-ye Malli-ye Ettelaat (The National Information Network)." *The National Center of Cyberspace*. The Supreme Council of Cyberspace, 26 June 2016. Web. 02 June 2017. <http://majazi.ir/page/national-information-network>.

Raisi, Ebrahim. *Instagram*, 05 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BU-FPZ9F9tT>.

—— *Instagram*, 15 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVhSdh4l4G5>.

—— *Instagram*, 15 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVX6xF8FEt2>.

—— *Instagram*, 28 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTbfC8yF2f6>.

—— *Telegram*, 02 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1436>.

—— *Telegram*, 05 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1496>.

—— *Telegram*, 05 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/2238>.

—— *Telegram*, 07 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1567>.

—— *Telegram*, 09 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1658>.

—— *Telegram*, 10 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1702>.

—— *Telegram*, 10 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1709>.

—— *Telegram*, 10 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1709>.

—— *Telegram*, 12 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1734>.

—— *Telegram*, 12 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1741>.

—— *Telegram*, 12 May 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1759>.

—— *Telegram*, 24 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1187>.

—— *Telegram*, 26 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1229>.

—— *Telegram*, 28 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1254>.

—— *Telegram*, 28 Apr. 2017. Web. 02 Sept 2017. <https://t.me/raisi_org/1258>.

Rasaee, Hamid. *Instagram*, 07 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVDi6hhDo7q>.

—— *Instagram*, 19 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVg9LL_g5qZ>.

—— *Telegram*, 01 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4404>.

—— *Telegram*, 15 May 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4453>.

—— *Telegram*, 16 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4806>.

—— *Telegram*, 16 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4809>.

—— *Telegram*, 17 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4838>.

—— *Telegram*, 19 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4854>.

—— *Telegram*, 20 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4862>.

—— *Telegram*, 20 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4863>.

—— *Telegram*, 23 May 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4404>.

—— *Telegram*, 25 May 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4637>.

—— *Telegram*, 30 June 2017. Web. 02 Sept 2017. <https://t.me/www_rasaee_ir/4926>.

RCILA. "Ghanun-e Asasi-ye Jomhuri-ye Eslami (The Constitution of the Islamic Republic of Iran)." *The Research Center of the Islamic Legislative Assembly*. Web. 05 June 2017. <http://rc.majlis.ir/fa/content/iran_constitution>.

—— "Ghanun-e Entekhabat-e Majlis-e Shoaray-ye Eslami (Islamic Consultative Assembly Elections Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/93241>.

—— "Ghanun-e Entekhabat-e Riasat-e Jomhuri-ye Eslami-ye Iran (The IRI Presidential Elections Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/91088>.

—— "Ghanun-e Hemayat-e az Hoghugh-e Padidavarandegan-e Narmafzarha-ye Rayaneh-i (The Law to Protect the Copyrights of Software Developers)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/93463>.

—— "Ghanun-e Jarayem-e Rayaneh-yi (The Cybercrime Law)." *The Research Center of the Islamic Legislative Assembly*. 24 June 2009. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/135717>.

—— "Ghanun-e Matbuat (The Press Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 05 June 2017. <http://rc.majlis.ir/fa/law/show/91180>.

—— "Ghanun-e Mojazat-e Enteshar va Efshaye Asnad-e Mahramaneh va Seri-ye Dolati (The Penal Law on the Leaking and Publishing of Secret and Confidential Governmental Material)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/97196>.

—— "Ghanun-e Mojazat-e Ghachagh-e Aslaheh va Mohemmat va Darandegan-e Selah va Mohemmat-e Gheir-e Mojaz (Penal Law on Smuggling and Illegal Ownership of Arms and Ammunition)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/797924>.

—— "Ghanun-e Nahve-ye Mojazat-e Ashkhasi keh dar Omur-e Samie va Basari Fa'aliatha-ye Gheir-e Mojaz Minemayand (Penal Law on the Illegal Activity in the Domain of Audio-Video Materials)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/130025>.

—— "Ghanun-e Tejarat-e Electronic-i (The Law on Electronic Commerce)." *The Research Center of the Islamic Legislative Assembly*. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/93997>.

—— "Mogharrarat Va Zavabet-e Shabakeha-ye Ettelaaresani-ye Rayaneh-i (Rules and Regulations for Computer Information Networks)." *The Research Center of the Islamic Legislative Assembly*. 03 Dec. 2001. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/100746>.

—— "Tashkil-e Committee-ye Tayin-e Masadighe-e Paygahha-ye Ettelaaresani-ye Rayaneh-i Gheyr-e Mojaz (Establishment of the Committee for Determining Incidences of Unauthorized Computer Information Networks)." *The Research Center of the Islamic Legislative Assembly*. 31 Dec. 2002. Web. 03 June 2017. <http://rc.majlis.ir/fa/law/show/101083>.

Rouhani, Hassan. "Didgah-haye Raees-e Jomhur-e Montakhab Darbareh-ye Filtering, Faza-ye Majazi Va Donyaye Ertebatat (The President-elect's Viewpoints about Filtering, Cyberspace and Communication World)." *Information Technology News Agency (ITNA)*. 01 July 2013. Web. 10 Dec. 2016. <http://itna.ir/fa/doc/interview/26665>.

—— *Instagram*, 01 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTithR9lzSP>.

—— *Instagram*, 02 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTl94CnlJrx>.

—— *Instagram*, 05 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTuTxucF3Kv>.

—— *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTzZWToFzwf>.

—— *Instagram*, 08 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BSoZHKLlrZD>.

—— *Instagram*, 08 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT1rr7UFR1Q>.

—— *Instagram*, 08 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT27yYbFtWQ>.

—— *Instagram*, 13 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUC0hwsFK6r>.

—— *Instagram*, 15 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUH3nBWFxCc>.

—— *Instagram*, 16 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BS9KIrPF1Om>.

—— *Instagram*, 17 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BUNRauTFzbf>.

—— *Instagram*, 18 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTBcasml-2b>.

—— *Instagram*, 29 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BV6kB9PFO33>.

—— *Official Website of the President of the Islamic Republic of Iran*, 14 June 2017. Web. 07 Apr. 2018. <http://www.president.ir/fa/99408>.

—— *Telegram*, 15 Apr. 2017. Web. 02 Sept 2017. <https://t.me/president_iran/4249>.

TNA. "Motor-e Jostejugar-e Parsijoo Dar Yazd Runamayi Shod (Parsijoo Search Engine Is Released in Yazd)." *Tasnim News Agency*. 04 Feb. 2015. Web. 02 June 2017. <https://www.tasnimnews.com/fa/news/1393/11/15/644626/>.

UNODC. "Ghanun-e Mojazat-e Eslami (The Islamic Penal Law)." *The United Nations Office on Drugs and Crime (UNODC)*. Web. 03 June 2017. <https://www.unodc.org/tldb/pdf/Islamic_Penal_Code_in_Farsi.pdf>.

WGDICC. "Fehrest-e Masadigh-e Mohtava-ye Mojremaneh (The List of Criminal Content Incidences)." *Working Group for Determining Incidences of Criminal Content*. Web. 03 June 2017. <http://internet.ir/crime_index.html>.

Yaminpour, Vahid. *Instagram*, 01 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTlDrA7gV8z>.

—— *Instagram*, 07 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTy3h6jgR4g>.

—— *Instagram*, 12 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BT_Kpk_gaYf>.

—— *Instagram*, 18 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVfmtwJlL5K>.

—— *Instagram*, 24 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTR1evpj1WX>.

—— *Telegram*, 23 May 2017. Web. 02 Sept 2017. <https://t.me/yaminpour/698>.

—— *Telegram*, 23 May 2017. Web. 02 Sept 2017. <https://t.me/yaminpour/699>.

—— *Telegram*, 30 May 2017. Web. 02 Sept 2017. <https://t.me/yaminpour/712>.

Zibakalam, Sadegh. *Instagram*, 02 May 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTmrn9AD090/>.

—— *Instagram*, 08 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVEboyQD4jW/>.

—— *Instagram*, 08 June 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BVEboyQD4jW/>.

—— *Instagram*, 22 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTN0SL7Dq7P/>.

—— *Instagram*, 27 Apr. 2017. Web. 02 Sept 2017. <https://www.instagram.com/p/BTaq7l1DIug/>.

—— *Telegram*, 09 May 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1556>.

—— *Telegram*, 26 June 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1515>.

—— *Telegram*, 26 June 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1673>.

—— *Telegram*, 30 June 2017. Web. 02 Sept 2017. <https://t.me/sadeghZibakalam/1684>.

APPENDICES

Appendix 1: A Sample List of the Cyber Activities Punishable Under the Iranian Laws

	Socio-cultural Category		
	The Crime	The Law	The Punishment
1	Insulting the religion of Islam and its sanctities, or any one of the great prophets (Noah, Abraham, Moses, Jesus, and Mohammad), the twelve imams of Shi'a Islam, and the daughter of the Prophet Mohammad	Article 513 of the Islamic Penal Law	Based on the severity of the insult, the accused can be sentenced from a minimum of 1 to 5 years in prison up to a maximum of the death penalty.
2	Intimidating or encouraging the commitment of obscenity or crime against public decency	Article 639 of the Islamic Penal Law	1 to 10 years in prison
		Article 15 of the Digital Crimes Law	2 to 20 million rials in fines OR 91 days to 1 year in prison
3	Publishing, distributing, and trading content that is against public decency	Article 14 of the Digital Crimes Law	The law distinguishes between those who commit these acts as professionals in a systematic fashion versus those who do so as non-professional and in a limited manner. Non-professionals are sentenced to 1 to 40 million rials in fines OR 91 days to 2 years in prison. Professionals can be sentenced to a minimum of 40 million rials in fines and 2 years in prison up to a maximum of the death penalty.
4	Online gambling	Article 705 of the Islamic Penal Law	1 month to 6 months OR 74 lashes
	Political Category		
	The Crime	The Law	The Punishment
5	Insulting the founder of the Islamic Revolution, the Ayatollah Ruhollah Khomeini, distorting his legacy, and insulting the office supreme leader.	Article 516 of the Islamic Penal Law	6 months to 2 years in prison
6	Spreading propaganda against the Islamic Republic of Iran or propaganda in favour of groups and organisations opposing the IRI	Article 500 of the Islamic Penal Law	3 months to 1 year in prison

7	Insulting and degrading governmental officials, institutions, and organisations	Article 609 of the Islamic Penal Law	3 months to 6 months OR up to 74 lashes OR 50,000 to 1 million rials in fines
8	Libeling governmental officials, institutions, and organisations	Article 697 of the Islamic Penal Law	1 month to 1 year in prison OR up to 74 lashes
9	Spreading falsehoods and disturbing the public opinion against governmental officials, institutions, and organisations	Article 698 of the Islamic Penal Law	2 months to 2 years in prison OR up to 74 lashes
10	Encouraging the people to boycott elections	Article 66 of Islamic Consultative Assembly Elections Law and Article 33 of the Presidential Elections Law	1 to 3 months in prison OR 1 to 5 million rials in fines AND an 8 year ban on membership in election executive and supervision councils
	Security Category		
	The Crime	The Law	The Punishment
11	Publishing content that involves a bomb threat	Article 511 of the Islamic Penal Law	Compensate the costs incurred by the threat and 6 months to 2 years in prison
12	Publishing content that incites people to war against and the killing of one another	Article 512 of the Islamic Penal Law	1 year to 5 years in prison
13	Publishing content that incites military forces to dereliction of duty, desertion, or surrender	Article 514 of the Islamic Penal Law	The law distinguishes between content deemed as effective versus ineffective in terms of the level of incitement. In the case of effective content the accused can be sentenced from a minimum of 2 to 10 years in prison up to a maximum of the death penalty, depending on the severity of the incitement. In the case of ineffective content the accused can be sentenced from 6 months to 3 years in prison.
14	Forming a group with the goal of acting against national security	Article 498 of the Islamic Penal Law	Based on the severity of the action, the accused can be sentenced from a minimum of 2 to 10 years in prison up to a maximum of the death penalty.
		Article 3 of the Digital Crimes Law	10 to 60 million rials in fines OR 91 days to 15 years in prison

15	Leaking and publishing secret governmental material	Article 2 and 3 of the Penal Law on the Leaking and Publishing of Secret and Confidential Governmental Material	3 months to 10 years in prison
16	Selling, advertising, distributing, and any type of trading of arms and ammunition	Article 5 of the Penal Law on Smuggling and Illegal Ownership of Arms and Ammunition	6 months to 15 years in prison
	Cyber Criminal Category		
	The Crime	The Law	The Punishment
17	Publishing, distributing, or trading software exclusively used for cybercrime	Article 25 of the Digital Crimes Law	91 days to 1 year in prison OR 5 to 20 million rials in fines
18	Selling, publishing, making accessible passwords and data that creates the possibility of unauthorised access to governmental or public digital systems	Article 25 of the Digital Crimes Law	91 days to 1 year in prison OR 5 to 20 million rials in fines
19	Publishing or making accessible knowledge on how to commit illegal entry, unauthorised surveillance, cyber espionage, and cyber sabotage against governmental or public digital systems	Article 25 of the Digital Crimes Law	91 days to 1 year in prison OR 5 to 20 million rials in fines
20	Making accessible or facilitating knowledge for the purpose of committing any type of cybercrime	Article 25 of the Digital Crimes Law	91 days to 1 year in prison OR 5 to 20 million rials in fines
21	Misrepresenting illegal audio-media material as legal and illegally reproducing legal material in violation of the copyright of the owner	Article 1 of the Penal Law Illegal Activity in the Domain of Audio-Video Materials	2 to 20 million rials in fines
22	Commercial activity in the area of the production and distribution audio-video materials without authorisation from the Ministry of Culture and Islamic Guidance	Article 2 of the Penal Law Illegal Activity in the Domain of Audio-Video Materials	10 to 100 million rials in fines

23	Infringing on the copyrights of software developers	Article 13 of the Law to Protect the Copyrights of Software Developers	The payment of damages to compensate software developers for losses due to copyright infringement AND 10 to 50 million rials in fines
24	Digital Fraud	Article 67 of the Law on Electronic Commerce	Full refund AND 1 year to 3 years in prison
25	Digital forgery	Article 68 of the Law on Electronic Commerce	1 year to 3 years and 50 million rials in fines
26	Infringing on consumer right and violating advertising rules	Article 69 and Article 70 of the Law on Electronic Commerce	10 to 100 million rials in fines
27	Unauthorised access to personal data	Article 71-73 of the Law on Electronic Commerce	The law distinguishes between premeditated and unpremeditated access to personal data. Premeditated cases can receive 1 to 3 years in prison, while unpremeditated cases can receive 3 months to 1 year in prison AND 50 million rials in fines
28	Infringing on copyrights	Article 74 of the Law on Electronic Commerce	3 months to 1 year in prison AND 50 million rials in fines
29	Illegally accessing to use or leak trade secrets	Article 75 of the Law on Electronic Commerce	6 months to 2.5 years in prison AND 50 million rials in fines
30	Infringing on trademarks	Article 76 of the Law on Electronic Commerce	1 year to 3 years in prison and 20 to 100 million rials in fines
	Sources		
1	UNODC. “Ghanun-e Mojazat-e Eslami (The Islamic Penal Law).” *The United Nations Office on Drugs and Crime (UNODC)*. Web. 3 June 2017. < https://www.unodc.org/tldb/pdf/Islamic_Penal_Code_in_Farsi.pdf >.		
2	RCILA. “Ghanun-e Jaraem-e Rayaneh-i (The Digital Crimes Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/135717 >.		
3	RCILA. “Ghanun-e Tejarat-e Electronic-i (The Law on Electronic Commerce)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/93997 >.		

4	RCILA. “Ghanun-e Hemayat-e az Hoghugh-e Padidavarandegan-e Narmafzarha-ye Rayaneh-i (The Law to Protect the Copyrights of Software Developers)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/93463 >.
5	RCILA. “Ghanun-e Mojazat-e Enteshar va Efshaye Asnad-e Mahramaneh va Seri-ye Dolati (The Penal Law on the Leaking and Publishing of Secret and Confidential Governmental Material)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/97196 >.
6	RCILA. “Ghanun-e Mojazat-e Enteshar va Efshaye Asnad-e Mahramaneh va Seri-ye Dolati (Penal Law on Smuggling and Illegal Ownership of Arms and Ammunition)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/797924 >.
7	RCILA. “Ghanun-e Nahve-ye Mojazat-e Ashkhasi keh dar Omur-e Samie va Basari Fa’aliatha-ye Gheir-e Mojaz Minemayand (Penal Law on the Illegal Activity in the Domain of Audio-Video Materials)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/130025 >.
8	RCILA. “Ghanun-e Entekhabat-e Majlis-e Shoaray-ye Eslami (Islamic Consultative Assembly Elections Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/93241 >.
9	RCILA. “Ghanun-e Entekhabat-e Riasat-e Jomhuri-ye Eslami-ye Iran (The IRI Presidential Elections Law)." *The Research Center of the Islamic Legislative Assembly*. Web. 3 June 2017. < http://rc.majlis.ir/fa/law/show/91088 >.

Appendix 2: The E-readiness Index Data

1. E-readiness Index											
	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
World Average	6.27	5.43	5.78	5.87	5.81	5.82	6.02	6.24	6.39	6.13	6.03
Israel	7.80	6.71	6.79	6.96	7.06	7.45	7.59	7.58	7.61	7.09	6.96
Turkey	5.50	4.51	4.37	4.63	4.51	4.58	4.77	5.61	5.64	5.34	5.24
UAE	…	…	…	…	…	…	6.32	6.22	6.09	6.12	6.25
Saudi Arabia	5.50	3.80	3.77	4.10	4.38	4.38	4.67	5.05	5.23	4.88	4.75
Egypt	4.60	3.88	3.76	3.72	4.08	3.90	4.14	4.26	4.81	4.33	4.21
Pakistan	4.00	2.66	2.78	2.74	2.61	2.93	3.03	3.79	4.10	3.50	3.55
Iran	3.30	3.30	3.20	3.40	3.68	3.08	3.15	3.08	3.29	3.43	3.24
Azerbaijan	…	2.72	2.38	2.37	2.43	2.72	2.92	3.26	3.18	2.97	3.00
Kazakhstan	3.50	2.76	2.55	2.52	2.60	2.97	3.22	3.78	3.89	3.31	3.44
Jordan	…	…	…	…	…	…	4.22	4.77	5.03	4.92	4.76
2025 Vision Targeted Countries' Average	4.89	3.79	3.70	3.81	3.92	4.00	4.40	4.74	4.89	4.59	4.54

1.1 Connectivity and Technology Infrastructure Sub-index								
	2003	2004	2005	2006	2007	2008	2009	2010
Israel	5.90	5.87	6.85	7.35	8.00	7.70	7.40	6.30
Turkey	3.40	3.00	3.30	3.60	4.00	4.40	4.85	4.20
UAE	…	…	…	5.00	5.20	5.20	6.05	6.80
Saudi Arabia	2.70	2.56	2.90	3.25	3.80	4.50	4.30	4.25
Egypt	1.90	1.72	2.20	2.65	2.75	3.40	3.00	2.55
Pakistan	1.10	0.55	1.25	1.50	2.90	2.90	2.85	2.35
Iran	2.00	2.34	2.35	2.70	2.80	3.15	3.50	3.20
Azarbaijan	1.30	0.73	1.70	1.85	2.70	2.70	2.95	2.85
Kazakhstan	1.30	0.98	1.70	2.10	2.40	3.30	3.40	3.15
Jordan	…	…	…	2.45	3.40	4.00	3.30	3.00
2025 Vision Targeted Countries' Average	2.45	2.22	2.78	3.25	3.80	4.13	4.16	3.87

1.2. Business Environment Sub-index								
	2003	2004	2005	2006	2007	2008	2009	2010
Israel	7.50	7.32	7.67	7.73	7.61	7.65	7.18	7.39
Turkey	6.10	5.76	6.49	6.68	6.66	6.60	5.94	6.11
UAE	…	…	…	7.68	7.54	7.64	7.10	7.27
Saudi Arabia	6.20	5.84	6.27	6.43	6.37	6.59	6.16	6.34
Egypt	5.30	5.28	5.48	5.84	6.04	6.36	6.23	6.20
Pakistan	5.30	4.93	5.20	5.12	5.34	5.42	4.81	5.31
Iran	4.80	4.39	4.61	4.66	4.17	4.40	4.22	4.14
Azarbaijan	5.30	5.23	5.29	5.54	5.39	5.41	4.70	4.93
Kazakhstan	5.40	5.26	5.37	5.37	5.93	5.66	4.82	5.26
Jordan	…	…	…	5.68	6.27	6.53	5.99	6.12
2025 Vision Targeted Countries' Average	5.74	5.50	5.80	6.07	6.13	6.23	5.72	5.91

1.3. Social and Cultural Environment Sub-index								
	2003	2004	2005	2006	2007	2008	2009	2010
Israel	8.80	8.75	8.00	8.00	7.20	7.93	7.50	7.50
Turkey	5.80	5.75	4.40	4.40	6.00	6.20	5.93	5.80
UAE	…	…	…	6.20	6.00	5.93	5.67	5.47
Saudi Arabia	5.50	5.00	4.00	4.20	4.80	5.33	5.50	5.13
Egypt	4.00	4.25	4.00	4.20	5.00	5.20	5.17	5.00
Pakistan	2.50	2.50	3.20	3.20	3.00	3.40	3.13	2.80
Iran	4.80	4.75	4.00	4.00	4.60	4.87	5.23	4.90
Azarbaijan	2.50	3.00	2.80	2.80	3.00	3.20	3.03	3.17
Kazakhstan	3.30	3.50	3.60	3.60	4.20	3.80	4.00	3.93
Jordan	…	…	…	5.00	5.40	5.53	5.63	5.30
2025 Vision Targeted Countries' Average	4.65	4.69	4.25	4.56	4.92	5.14	5.08	4.90

1.4. Legal Environment Sub-index								
	2003	2004	2005	2006	2007	2008	2009	2010
Israel	7.10	7.32	7.24	7.18	7.00	7.00	7.15	7.05
Turkey	4.90	4.65	4.71	4.97	5.10	5.40	5.45	5.45
UAE	…	…	…	6.97	5.55	5.50	5.00	5.10
Saudi Arabia	3.60	4.29	4.42	4.89	4.80	5.00	4.75	4.75
Egypt	4.80	4.90	4.74	4.94	4.00	5.20	5.20	5.20
Pakistan	3.50	3.54	3.80	3.90	4.65	5.30	5.60	5.90
Iran	4.50	3.87	2.70	2.49	2.10	2.20	3.00	3.00
Azarbaijan	2.10	2.12	2.34	2.68	2.60	2.60	3.25	3.40
Kazakhstan	2.30	2.27	2.83	3.42	3.40	3.70	3.45	3.45
Jordan	…	…	…	5.03	5.10	5.20	4.90	4.90
2025 Vision Targeted Countries' Average	4.10	4.12	4.10	4.65	4.43	4.71	4.78	4.82

1. 5. Government Policy and Vision Sub-index								
	2003	2004	2005	2006	2007	2008	2009	2010
Israel	8.80	8.75	8.75	8.75	7.05	7.40	6.90	7.05
Turkey	5.50	5.50	5.25	5.25	5.75	5.75	5.35	5.50
UAE	…	…	…	7.75	6.45	6.45	6.35	6.20
Saudi Arabia	4.30	5.00	5.00	5.00	6.05	6.05	5.50	4.85
Egypt	5.00	5.50	4.25	4.25	5.10	5.45	4.90	4.90
Pakistan	2.80	2.75	2.75	3.50	3.90	4.25	3.80	4.30
Iran	4.30	4.00	3.25	3.25	2.50	2.50	2.65	2.40
Azarbaijan	1.50	2.25	3.00	3.25	2.85	2.85	2.70	2.55
Kazakhstan	1.80	2.50	3.25	3.50	2.85	2.85	3.10	3.93
Jordan	…	…	…	5.00	5.25	5.60	5.90	5.45
2025 Vision Targeted Countries' Average	4.25	4.53	4.44	4.95	4.78	4.92	4.72	4.71

1.6. Consumer and Business Adoption Sub-index								
	2003	2004	2005	2006	2007	2008	2009	2010
Israel	5.80	6.42	7.40	7.45	8.00	7.70	6.63	6.83
Turkey	3.40	3.88	4.15	4.35	6.15	5.75	4.98	4.98
UAE	…	…	…	5.85	6.50	6.00	6.18	6.18
Saudi Arabia	3.10	4.65	4.45	4.80	4.90	4.55	3.90	3.90
Egypt	3.10	4.74	3.65	3.65	3.55	4.25	3.05	3.05
Pakistan	1.80	2.21	1.95	1.95	3.65	4.10	2.45	2.51
Iran	1.70	3.65	2.00	2.05	2.50	2.25	2.48	2.33
Azarbaijan	1.00	1.60	1.60	1.80	3.10	3.10	1.98	1.98
Kazakhstan	1.00	1.58	1.70	1.95	4.05	4.05	1.98	1.98
Jordan	…	…	…	3.60	4.15	4.25	4.55	4.55
2025 Vision Targeted Countries' Average	2.61	3.59	3.36	3.75	4.66	4.60	3.82	3.83

The data for the e-readiness index and its respective sub-indexes has been extracted from the following reports:

- "Digital Economy Rankings 2010: Beyond E-readiness Economist." *The Economist Intelligence Unit.* 2010. Web. 1 Mar. 2017. <http://graphics.eiu.com/upload/EIU_Digital_economy_rankings_2010_FINAL_WEB.pdf>.
- "E-readiness Rankings 2009: The Usage Imperative." *The Economist Intelligence Unit*. 2009. Web. 1 Mar. 2017. <http://graphics.eiu.com/pdf/E-readiness%20rankings.pdf>.
- "E-readiness Rankings 2008: Maintaining Momentum." *The Economist Intelligence Unit*. 2008. Web. 1 Mar. 2017. <http://www-05.ibm.com/ie/pdf/ibm_ereadiness_2008.pdf >.
- "The 2007 E-readiness Rankings: Raising the Bar." *The Economist Intelligence Unit*. 2007. Web. 1 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/2007Ereadiness_Ranking_WP.pdf>.
- "The 2006 E-readiness Rankings." *The Economist Intelligence Unit*. 2006. Web. 1 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/2006Ereadiness_Ranking_WP.pdf>.
- "The 2005 E-readiness Rankings." *The Economist Intelligence Unit*. 2005. Web. 1 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/2005Ereadiness_Ranking_WP.pdf>.
- "The 2004 E-readiness Rankings." *The Economist Intelligence Unit*. 2004. Web. 1 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/ERR2004.pdf>.

- "The 2003 E-readiness Rankings." *The Economist Intelligence Unit*. 2003. Web. 1 Mar. 2017. <http://graphics.eiu.com/files/ad_pdfs/eready_2003.pdf>.
- "The 2002 E-readiness Rankings." *The Economist Intelligence Unit*. 2002. Web. 1 Mar. 2017. <http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN010005.pdf>.
- "The Economist Intelligence Unit / Pyramid Research E-readiness Rankings." *The Economist Intelligence Unit*. 2001. Web. 1 Mar. 2017. <https://web.archive.org/web/20071013015357/http://www.ladlass.com/ice/archives/files/E-Readiness_from_Economist%202001.pdf>.
- "The EIU's E-business Readiness Rankings." *The Economist Intelligence Unit*. 2000. Web. 1 Mar. 2017. <https://web.archive.org/web/20011121105637/http://www.ebusinessforum.com/index.asp?layout=rich_story&doc_id=3331&country_id=&title=The+EIU%27s+e-business+readiness+rankings,+May+2000&channelid=6&categoryid=20>.

Appendix 3: The E-Government Development Index Data

2. E-Government Development Index (EGDI)								
	2003	2004	2005	2008	2010	2012	2014	2016
World Average	0.40	0.41	0.43	0.45	0.44	0.49	0.47	0.49
Iran	0.33	0.33	0.38	0.41	0.42	0.49	0.45	0.46
Afghanistan	0.12	0.13	0.15	0.20	0.21	0.17	0.19	0.23
Armenia	0.38	0.39	0.36	0.42	0.40	0.50	0.59	0.52
Azerbaijan	0.36	0.39	0.38	0.46	0.46	0.50	0.55	0.63
Bahrain	0.51	0.53	0.53	0.57	0.74	0.69	0.81	0.77
Egypt	0.24	0.27	0.38	0.48	0.45	0.46	0.51	0.46
Georgia	0.35	0.38	0.40	0.46	0.42	0.56	0.60	0.61
Iraq	0.32	0.36	0.33	0.27	0.30	0.34	0.31	0.33
Israel	0.66	0.68	0.69	0.74	0.66	0.81	0.82	0.78
Jordan	0.43	0.44	0.46	0.55	0.53	0.49	0.52	0.51
Kazakhstan	0.39	0.43	0.48	0.47	0.56	0.68	0.73	0.73
Kuwait	0.37	0.37	0.44	0.52	0.53	0.60	0.63	0.71
Kyrgyzstan	0.33	0.45	0.44	0.42	0.44	0.49	0.47	0.50
Lebanon	0.42	0.42	0.46	0.48	0.44	0.51	0.50	0.56
Oman	0.36	0.29	0.34	0.47	0.46	0.59	0.63	0.60
Pakistan	0.25	0.30	0.28	0.32	0.28	0.28	0.26	0.26
Qatar	0.41	0.40	0.49	0.53	0.49	0.64	0.64	0.67
Saudi Arabia	0.34	0.39	0.41	0.49	0.51	0.67	0.69	0.68
Syrian Arab Republic	0.26	0.26	0.29	0.36	0.31	0.37	0.31	0.34
Tajikistan	0.30	0.31	0.33	0.32	0.35	0.41	0.34	0.34
Turkey	0.51	0.49	0.50	0.48	0.48	0.53	0.54	0.59
Turkmenistan	0.34	0.34	0.32	0.33	0.32	0.38	0.35	0.33
United Arab Emirates	0.54	0.47	0.57	0.63	0.53	0.73	0.71	0.75
Uzbekistan	0.32	0.40	0.41	0.41	0.45	0.51	0.47	0.54
Yemen	0.19	0.20	0.21	0.21	0.22	0.25	0.27	0.22
2025 Vision Targeted Countries' Average	0.36	0.38	0.40	0.44	0.44	0.51	0.52	0.53

2.1. Telecommunications Infrastructure Index (TII)								
	2003	2004	2005	2008	2010	2012	2014	2016
Iran	0.09	0.09	0.11	0.17	0.21	0.26	0.29	0.35
Afghanistan	0.00	0.00	0.00	0.02	0.03	0.06	0.15	0.11
Armenia	0.07	0.07	0.08	0.09	0.13	0.32	0.39	0.39
Azerbaijan	0.08	0.08	0.07	0.11	0.13	0.30	0.46	0.49
Bahrain	0.35	0.33	0.32	0.33	0.58	0.42	0.71	0.78
Egypt	0.06	0.07	0.07	0.09	0.12	0.22	0.36	0.30
Georgia	0.12	0.10	0.11	0.11	0.12	0.23	0.43	0.42
Iraq	0.02	0.02	0.02	0.01	0.05	0.12	0.22	0.16
Israel	0.45	0.42	0.40	0.61	0.43	0.69	0.72	0.62
Jordan	0.09	0.10	0.10	0.17	0.18	0.27	0.31	0.35
Kazakhstan	0.06	0.06	0.06	0.13	0.18	0.36	0.57	0.57
Kuwait	0.23	0.23	0.27	0.28	0.25	0.42	0.59	0.74
Kyrgyzstan	0.04	0.04	0.04	0.05	0.09	0.19	0.38	0.31
Lebanon	0.19	0.18	0.19	0.19	0.19	0.27	0.40	0.49
Oman	0.13	0.14	0.14	0.16	0.21	0.39	0.49	0.51
Pakistan	0.03	0.03	0.02	0.05	0.08	0.12	0.12	0.13
Qatar	0.31	0.30	0.31	0.35	0.31	0.45	0.59	0.60
Saudi Arabia	0.12	0.14	0.14	0.21	0.40	0.43	0.55	0.57
Syrian Arab Republic	0.04	0.04	0.05	0.09	0.12	0.20	0.20	0.21
Tajikistan	0.05	0.04	0.04	0.02	0.06	0.15	0.23	0.19
Turkey	0.19	0.17	0.16	0.22	0.26	0.35	0.36	0.38
Turkmenistan	0.04	0.04	0.04	0.04	0.04	0.11	0.22	0.26
United Arab Emirates	0.44	0.39	0.36	0.38	0.54	0.56	0.59	0.69
Uzbekistan	0.05	0.05	0.05	0.04	0.08	0.21	0.23	0.25
Yemen	0.04	0.04	0.04	0.03	0.03	0.10	0.12	0.15
2025 Vision Targeted Countries' Average	0.13	0.13	0.13	0.16	0.19	0.29	0.39	0.40

2.2 Online Service Index (OSI)								
	2003	2004	2005	2008	2010	2012	2014	2016
Iran	0.15	0.16	0.30	0.26	0.27	0.49	0.37	0.33
Afghanistan	0.08	0.13	0.18	0.27	0.24	0.24	0.18	0.30
Armenia	0.14	0.25	0.11	0.27	0.18	0.33	0.61	0.43
Azerbaijan	0.13	0.20	0.18	0.39	0.33	0.37	0.43	0.68
Bahrain	0.33	0.41	0.42	0.52	0.74	0.86	0.94	0.83
Egypt	0.04	0.10	0.45	0.61	0.54	0.60	0.59	0.47
Georgia	0.05	0.15	0.21	0.35	0.25	0.60	0.60	0.64
Iraq	0.00	0.12	0.05	0.11	0.16	0.29	0.20	0.36
Israel	0.63	0.69	0.73	0.67	0.57	0.85	0.87	0.86
Jordan	0.42	0.35	0.43	0.61	0.54	0.39	0.52	0.46
Kazakhstan	0.19	0.32	0.45	0.32	0.54	0.78	0.75	0.77
Kuwait	0.14	0.14	0.25	0.41	0.47	0.58	0.57	0.65
Kyrgyzstan	0.07	0.39	0.37	0.30	0.32	0.42	0.28	0.43
Lebanon	0.25	0.24	0.34	0.39	0.27	0.48	0.35	0.51
Oman	0.26	0.05	0.17	0.48	0.38	0.67	0.73	0.59
Pakistan	0.30	0.48	0.43	0.42	0.25	0.37	0.32	0.33
Qatar	0.14	0.09	0.33	0.39	0.29	0.74	0.65	0.67
Saudi Arabia	0.18	0.31	0.38	0.46	0.32	0.80	0.77	0.67
Syrian Arab Republic	0.04	0.05	0.07	0.24	0.04	0.23	0.16	0.33
Tajikistan	0.00	0.00	0.06	0.04	0.09	0.24	0.06	0.12
Turkey	0.56	0.53	0.52	0.42	0.35	0.46	0.56	0.60
Turkmenistan	0.04	0.07	0.00	0.05	0.03	0.19	0.09	0.09
United Arab Emirates	0.42	0.31	0.61	0.72	0.26	0.86	0.88	0.89
Uzbekistan	0.00	0.23	0.27	0.27	0.39	0.50	0.45	0.69
Yemen	0.04	0.05	0.10	0.07	0.05	0.18	0.31	0.14
2025 Vision Targeted Countries' Average	0.18	0.23	0.30	0.36	0.31	0.50	0.49	0.51

2.3 Human Capital Index (HCI)								
	2003	2004	2005	2008	2010	2012	2014	2016
Iran	0.75	0.73	0.74	0.79	0.78	0.71	0.69	0.71
Afghanistan	0.27	0.27	0.27	0.33	0.36	0.22	0.24	0.28
Armenia	0.92	0.86	0.90	0.90	0.90	0.85	0.77	0.73
Azerbaijan	0.88	0.88	0.88	0.88	0.91	0.83	0.75	0.72
Bahrain	0.85	0.86	0.85	0.86	0.88	0.80	0.78	0.72
Egypt	0.62	0.63	0.62	0.73	0.69	0.56	0.59	0.60
Georgia	0.89	0.89	0.89	0.92	0.91	0.83	0.79	0.78
Iraq	0.93	0.93	0.93	0.69	0.69	0.62	0.53	0.48
Israel	0.91	0.93	0.94	0.95	0.94	0.89	0.85	0.86
Jordan	0.78	0.86	0.86	0.87	0.86	0.80	0.72	0.73
Kazakhstan	0.91	0.92	0.93	0.98	0.96	0.91	0.86	0.84
Kuwait	0.74	0.73	0.81	0.87	0.87	0.79	0.72	0.73
Kyrgyzstan	0.87	0.91	0.92	0.92	0.91	0.85	0.74	0.75
Lebanon	0.83	0.83	0.84	0.87	0.85	0.79	0.74	0.69
Oman	0.67	0.68	0.71	0.77	0.79	0.72	0.66	0.68
Pakistan	0.42	0.41	0.40	0.47	0.50	0.36	0.33	0.32
Qatar	0.79	0.82	0.83	0.85	0.88	0.73	0.67	0.73
Saudi Arabia	0.71	0.71	0.71	0.81	0.83	0.77	0.75	0.80
Syrian Arab Republic	0.71	0.70	0.75	0.75	0.77	0.69	0.58	0.49
Tajikistan	0.88	0.90	0.90	0.90	0.89	0.83	0.72	0.70
Turkey	0.77	0.77	0.80	0.81	0.83	0.77	0.71	0.79
Turkmenistan	0.92	0.92	0.93	0.90	0.90	0.84	0.75	0.66
United Arab Emirates	0.74	0.73	0.74	0.79	0.81	0.78	0.67	0.68
Uzbekistan	0.91	0.91	0.91	0.91	0.88	0.83	0.73	0.70
Yemen	0.48	0.49	0.50	0.54	0.57	0.46	0.38	0.38
2025 Vision Targeted Countries' Average	0.77	0.77	0.78	0.80	0.81	0.73	0.67	0.66

2.4 E-Participation Index (EPI)								
	2003	2004	2005	2008	2010	2012	2014	2016
Iran	0.03	0.03	0.03	0.09	0.07	0.18	0.29	0.20
Afghanistan	0.03	0.03	0.02	0.05	0.06	0.13	0.14	0.42
Armenia	0.05	0.03	0.06	0.05	0.04	0.00	0.53	0.53
Azerbaijan	0.02	0.02	0.02	0.25	0.17	0.13	0.43	0.68
Bahrain	0.05	0.05	0.05	0.34	0.67	0.66	0.82	0.75
Egypt	0.02	0.02	0.08	0.25	0.29	0.68	0.55	0.41
Georgia	0.02	0.02	0.02	0.05	0.06	0.21	0.59	0.56
Iraq	0.00	0.03	0.00	0.20	0.04	0.11	0.14	0.42
Israel	0.40	0.28	0.32	0.32	0.41	0.89	0.86	0.83
Jordan	0.17	0.05	0.05	0.55	0.29	0.11	0.47	0.46
Kazakhstan	0.10	0.13	0.21	0.09	0.56	0.95	0.76	0.59
Kuwait	0.02	0.02	0.00	0.07	0.23	0.18	0.43	0.64
Kyrgyzstan	0.03	0.21	0.16	0.14	0.43	0.29	0.41	0.59
Lebanon	0.09	0.08	0.11	0.41	0.27	0.32	0.29	0.49
Oman	0.26	0.00	0.02	0.20	0.16	0.45	0.71	0.56
Pakistan	0.16	0.16	0.13	0.09	0.17	0.13	0.33	0.37
Qatar	0.00	0.02	0.05	0.18	0.13	0.63	0.61	0.64
Saudi Arabia	0.03	0.05	0.06	0.32	0.10	0.63	0.57	0.71
Syrian Arab Republic	0.00	0.00	0.00	0.05	0.01	0.03	0.10	0.46
Tajikistan	0.00	0.00	0.00	0.00	0.03	0.00	0.12	0.20
Turkey	0.21	0.30	0.29	0.14	0.21	0.05	0.49	0.63
Turkmenistan	0.02	0.02	0.00	0.02	…	0.00	0.12	0.07
United Arab Emirates	0.17	0.05	0.13	0.30	0.13	0.74	0.84	0.75
Uzbekistan	0.00	0.02	0.03	0.09	0.31	0.24	0.24	0.68
Yemen	0.03	0.03	0.00	0.00	0.04	0.00	0.27	0.14
2025 Vision Targeted Countries' Average	0.08	0.07	0.07	0.17	0.20	0.31	0.44	0.51

The data for the E-Government Development Index and its respective sub-indexes has been extracted from the following reports:

- "UN E-Government Survey 2016." *The United Nations*. 2016. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016 >.
- "UN E-Government Survey 2014." *The United Nations*. 2014. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014 >.
- "UN E-Government Survey 2012." *The United Nations*. 2012. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2012 >.
- "UN E-Government Survey 2010." *The United Nations*. 2010. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2010 >.
- "UN E-Government Survey 2008." *The United Nations*. 2008. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2008 >.
- "UN E-Government Survey 2005." *The United Nations*. 2005. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2005 >.
- "UN E-Government Survey 2004." *The United Nations*. 2004. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2004 >.
- "UN E-Government Survey 2004." *The United Nations*. 2004. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2004 >.
- "UN E-Government Survey 2003." *The United Nations*. 2003. Web. 1 Mar. 2017. < https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2003 >.

Appendix 4: The Networked Readiness Index Data

3. Networked Readiness Index						
	2011	2012	2013	2014	2015	2016
World Average	3.91	3.96	3.97	4.01	4.07	4.14
Iran	3.41	3.36	3.43	3.42	3.6	3.7
Afghanistan	…	…	…	…	…	…
Armenia	3.24	3.49	3.76	4.03	4.2	4.3
Azerbaijan	3.79	3.95	4.11	4.31	4.3	4.3
Bahrain	4.64	4.90	4.83	4.86	4.9	5.1
Egypt	3.76	3.77	3.78	3.71	3.6	3.7
Georgia	3.45	3.60	3.93	4.09	4.2	4.3
Iraq	…	…	…	…	…	…
Israel	4.81	5.24	5.39	5.42	5.4	5.4
Jordan	4.00	4.17	4.20	4.36	4.3	4.2
Kazakhstan	3.80	4.03	4.32	4.58	4.5	4.6
Kuwait	3.74	3.95	3.94	3.96	4.0	4.2
Kyrgyz Republic	3.18	3.13	3.09	3.22	3.5	3.7
Lebanon	3.49	3.49	3.53	3.64	3.5	3.8
Oman	4.25	4.35	4.48	4.56	4.5	4.3
Pakistan	3.54	3.39	3.35	3.33	3.3	3.4
Qatar	4.79	4.81	5.10	5.22	5.1	5.2
Saudi Arabia	4.44	4.62	4.82	4.78	4.7	4.8
Syria	3.06	2.85	…	…	…	…
Tajikistan	3.23	3.19	3.29	…	3.2	3.3
Turkey	3.79	4.07	4.22	4.30	4.4	4.4
Turkmenistan	…	…	…	…	…	…
United Arab Emirates	4.80	4.77	5.07	5.20	5.3	5.3
Uzbekistan	…	…	…	…	…	…
Yemen	…	2.41	2.63	2.73	2.7	…
2025 Vision Targeted Countries' Average	3.86	3.88	4.06	4.20	4.16	4.32

3.1 Environment Sub-index						
	2011	2012	2013	2014	2015	2016
Iran	3.53	3.71	3.86	3.79	3.70	3.90
Afghanistan	…	…	…	…	…	…
Armenia	3.19	3.42	3.70	3.80	3.90	3.90
Azerbaijan	3.67	3.73	3.84	3.94	3.90	3.90
Bahrain	4.59	4.84	4.83	4.52	4.50	4.60
Egypt	3.79	3.68	3.62	3.44	3.30	3.50
Georgia	3.58	3.77	3.86	3.91	4.00	4.10
Iraq	…	…	…	…	…	…
Israel	4.79	4.98	4.97	4.97	5.00	5.00
Jordan	4.04	4.16	4.35	4.45	4.50	4.50
Kazakhstan	3.57	3.70	3.93	4.11	4.20	4.30
Kuwait	3.99	3.99	3.90	3.85	3.90	4.00
Kyrgyz Republic	3.20	2.99	3.02	3.39	3.60	3.70
Lebanon	3.62	3.64	3.74	4.69	3.50	3.80
Oman	4.17	4.63	4.61	3.44	4.50	4.20
Pakistan	3.48	3.42	3.42	3.44	3.40	3.40
Qatar	4.73	5.10	5.19	4.86	5.30	5.30
Saudi Arabia	4.53	5.00	4.87	4.86	4.80	4.90
Syria	3.09	3.33	…	…	…	…
Tajikistan	3.07	3.67	3.80	…	3.70	4.00
Turkey	3.87	4.06	4.31	4.38	4.40	4.20
Turkmenistan	…	…	…	…	…	…
United Arab Emirates	4.77	4.83	5.05	5.10	5.40	5.20
Uzbekistan	…	…	…	…	…	…
Yemen	…	2.86	2.91	2.94	2.90	…
2025 Vision Targeted Countries' Average	3.86	3.98	4.09	4.10	4.12	4.23

3.2 Readiness Sub-index						
	2011	2012	2013	2014	2015	2016
Iran	4.09	3.75	3.69	3.87	4.50	4.60
Afghanistan	…	…	…	…	…	…
Armenia	3.93	4.26	4.60	5.13	5.30	5.40
Azerbaijan	4.44	4.86	4.98	5.21	4.90	4.80
Bahrain	4.86	5.54	5.27	5.52	5.30	5.80
Egypt	4.13	4.54	4.41	4.35	4.30	4.20
Georgia	3.82	4.15	4.99	5.39	5.30	5.30
Iraq	…	…	…	…	…	…
Israel	4.90	5.32	5.59	5.76	5.40	5.50
Jordan	4.37	5.10	4.97	5.22	4.60	4.30
Kazakhstan	4.34	5.06	4.98	5.57	5.50	5.50
Kuwait	3.95	5.09	4.87	4.95	4.80	5.20
Kyrgyz Republic	3.68	3.93	3.78	3.95	4.60	4.70
Lebanon	4.03	4.31	4.29	4.63	4.10	4.50
Oman	4.81	4.74	4.92	5.07	4.90	4.80
Pakistan	4.28	4.03	4.11	3.97	3.60	4.00
Qatar	5.47	4.93	5.06	5.48	5.00	5.10
Saudi Arabia	4.91	5.14	5.23	5.11	4.70	5.00
Syria	3.74	2.86	…	…	…	…
Tajikistan	4.02	3.28	3.22	…	3.00	3.00
Turkey	4.07	4.86	5.27	5.35	5.30	5.50
Turkmenistan	…	…	…	…	…	…
United Arab Emirates	5.37	5.29	5.23	5.44	5.10	5.00
Uzbekistan	…	…	…	…	…	…
Yemen	…	2.71	3.24	3.31	3.10	…
2025 Vision Targeted Countries' Average	4.36	4.46	4.64	4.91	4.67	4.85

3.3 Usage Sub-index						
	2011	2012	2013	2014	2015	2016
Iran	2.60	3.05	3.06	3.05	3.10	3.30
Afghanistan	…	…	…	…	…	…
Armenia	2.61	3.24	3.44	3.65	3.90	4.00
Azerbaijan	3.26	3.73	3.99	4.24	4.30	4.40
Bahrain	4.45	4.77	4.83	5.13	5.20	5.30
Egypt	3.37	3.42	3.49	3.45	3.50	3.50
Georgia	2.96	3.21	3.46	3.63	3.80	4.10
Iraq	…	…	…	…	…	…
Israel	4.75	5.36	5.45	5.45	5.50	5.50
Jordan	3.57	3.77	3.79	3.96	4.10	4.10
Kazakhstan	3.49	3.61	4.18	4.39	4.40	4.40
Kuwait	3.27	3.55	3.94	4.00	4.10	4.30
Kyrgyz Republic	2.65	2.68	2.81	2.81	3.00	3.20
Lebanon	2.82	3.02	3.21	3.45	3.60	3.80
Oman	3.76	4.12	4.36	4.40	4.60	4.50
Pakistan	2.87	3.00	2.89	2.91	2.90	2.90
Qatar	4.16	4.79	5.35	5.33	5.40	5.40
Saudi Arabia	3.88	4.33	4.74	4.78	4.90	5.10
Syria	2.35	2.79	…	…	…	…
Tajikistan	2.60	2.81	3.12	…	2.90	2.90
Turkey	3.42	3.69	3.78	3.90	4.00	4.00
Turkmenistan	…	…	…	…	…	…
United Arab Emirates	4.27	4.52	5.07	5.24	5.60	5.60
Uzbekistan	…	…	…	…	…	…
Yemen	…	2.16	2.27	2.44	2.50	…
2025 Vision Targeted Countries' Average	3.36	3.60	3.86	4.01	4.07	4.23

3.4 Impact Sub-index					
	2012	2013	2014	2015	2016
Iran	2.93	3.09	2.97	3.00	3.20
Afghanistan	…	…	…	…	…
Armenia	3.05	3.31	3.53	3.90	3.90
Azerbaijan	3.48	3.65	3.85	4.00	4.00
Bahrain	4.44	4.39	4.26	4.50	4.50
Egypt	3.43	3.60	3.61	3.40	3.40
Georgia	3.26	3.39	3.44	3.80	5.30
Iraq	…	…	…	…	…
Israel	5.29	5.54	5.52	5.50	5.70
Jordan	3.66	3.70	3.81	4.10	3.90
Kazakhstan	3.73	4.18	4.26	4.10	4.20
Kuwait	3.17	3.04	3.04	3.20	3.40
Kyrgyz Republic	2.91	2.75	2.71	3.00	3.10
Lebanon	2.99	2.86	2.87	2.90	3.20
Oman	3.92	4.04	4.07	4.10	3.70
Pakistan	3.12	2.97	2.99	3.10	3.10
Qatar	4.43	4.80	4.84	4.80	4.90
Saudi Arabia	4.01	4.43	4.40	4.30	4.30
Syria	2.43	…	…	…	…
Tajikistan	2.99	3.03	…	3.20	3.20
Turkey	3.67	3.54	3.55	3.90	3.80
Turkmenistan	…	…	…	…	…
United Arab Emirates	4.42	4.94	5.01	5.20	5.20
Uzbekistan	…	…	…	…	…
Yemen	1.93	2.08	2.24	2.40	…
2025 Vision Targeted Countries' Average	3.49	3.67	3.74	3.82	4.00

The data for the Networked Readiness Index and its respective sub-indexes has been extracted from the following reports:

- "The Global Information Technology Report 2016: Innovating in the Digital Economy." *The World Economic Forum*. 2016. Web. 1 Mar. 2017. <https://www.weforum.org/reports/the-global-information-technology-report-2016>.
- "The Global Information Technology Report 2015: ICTs for Inclusive Growth." *The World Economic Forum*. 2015. Web. 1 Mar. 2017. <https://reports.weforum.org/global-information-technology-report-2015/>.
- "The Global Information Technology Report 2014: Rewards and Risks of Big Data." *The World Economic Forum*. 2014. Web. 1 Mar. 2017. <http://reports.weforum.org/global-information-technology-report-2014/>.
- "The Global Information Technology Report 2013: Growth and Jobs in a Hyperconnected World." *The World Economic Forum*. 2013. Web. 1 Mar. 2017. <http://reports.weforum.org/global-information-technology-report-2013/>.
- "The Global Information Technology Report 2012: Living in a Hyperconnected World." *The World Economic Forum*. 2012. Web. 1 Mar. 2017. <http://reports.weforum.org/global-information-technology-2012/>.
- "The Global Information Technology Report 2010–2011: Transformations 2.0." *The World Economic Forum*. 2011. Web. 1 Mar. 2017. <http://reports.weforum.org/global-information-technology-2011/ >.

Appendix 5: The ICT Development Index Data

4. ICT Development Index (IDI)									
	2002	2007	2008	2010	2011	2012	2013	2015	2016
World Average	2.52	3.32	3.62	4.14	4.15	4.6	4.77	4.74	4.94
Iran	1.93	2.73	2.96	3.48	3.61	4.02	4.29	4.66	4.99
Afghanistan	…	…	…	1.37	…	1.57	1.67	1.62	1.73
Armenia	2.03	2.66	2.94	4.10	4.18	4.89	5.08	5.34	5.6
Azerbaijan	1.71	2.77	2.97	4.21	4.62	5.22	5.65	6.23	6.28
Bahrain	3.30	4.95	5.16	5.42	5.79	7.22	7.4	7.76	7.91
Egypt	1.81	2.44	2.73	3.48	3.65	4.28	4.45	4.26	4.44
Georgia	2.13	2.87	2.96	3.76	4.24	4.48	4.86	5.33	5.59
Iraq	…	…	…	…	…	…	…	…	…
Israel	4.24	5.93	6.20	6.69	6.70	7.25	7.29	7.25	7.4
Jordan	2.36	2.98	3.29	3.82	3.90	4.48	4.62	4.67	5.06
Kazakhstan	2.18	3.17	3.39	4.81	5.41	5.80	6.08	6.42	6.57
Kuwait	2.77	3.54	…	5.64	…	…	…	6.45	6.54
Kyrgyz Republic	1.97	2.52	2.62	3.02	…	3.69	3.78	3.85	3.99
Lebanon	2.53	3.02	3.12	4.18	4.62	5.32	5.71	5.91	5.93
Oman	2.12	3.17	3.45	4.41	4.80	5.43	6.1	6.04	6.27
Pakistan	0.89	1.45	1.59	1.79	1.78	2.01	2.05	2.15	2.35
Qatar	2.84	4.25	4.50	6.10	6.41	6.46	7.01	6.78	6.9
Saudi Arabia	2.13	3.76	4.13	4.96	5.46	6.01	6.36	6.88	6.9
Syria	1.69	2.65	2.66	3.14	3.13	3.39	3.46	3.21	3.32
Tajikistan	1.76	2.11	…	…	…	…	…	…	…
Turkey	2.41	3.63	3.81	4.56	4.47	5.12	5.29	5.45	5.69
Turkmenistan	1.96	2.27	2.15	2.50	2.49	…	…	…	…
United Arab Emirates	3.27	5.20	5.63	5.38	5.68	6.27	7.03	6.96	7.11
Uzbekistan	1.75	2.06	2.22	2.55	3.02	3.27	3.4	3.76	4.05
Yemen	1.04	1.48	1.49	1.72	1.76	2.07	2.18	1.96	2.02
2025 Vision Targeted Countries' Average	2.21	3.11	3.33	3.96	4.29	4.68	4.94	5.13	5.30

4.1 Access Sub-index									
	2002	2007	2008	2010	2011	2012	2013	2015	2016
Iran	1.74	3.06	3.69	4.62	4.53	5.11	5.53	5.97	6.26
Afghanistan	…	…	…	1.92	…	2.23	2.44	2.39	2.51
Armenia	1.52	2.71	3.22	4.73	4.23	5.55	5.64	3.47	3.85
Azerbaijan	0.91	2.93	3.28	4.90	4.84	5.83	6.07	6.68	6.78
Bahrain	3.95	6.85	6.55	7.22	6.82	7.64	7.72	7.76	7.91
Egypt	1.55	2.55	3.23	4.30	4.00	4.99	5.09	5.20	5.30
Georgia	1.56	3.01	2.89	4.50	4.65	5.61	5.99	6.25	6.29
Iraq	…	…	…	…	…	…	…	…	…
Israel	5.71	7.01	6.93	7.73	7.38	8.21	8.31	8.18	8.28
Jordan	2.15	3.13	3.65	4.62	4.53	5.43	5.47	5.91	6.10
Kazakhstan	1.55	3.63	3.90	5.98	6.14	6.73	6.84	7.46	7.56
Kuwait	3.38	4.39	…	6.32	…	…	…	7.31	7.40
Kyrgyz Republic	1.05	2.02	2.07	3.20	…	4.01	4.05	4.16	4.25
Lebanon	2.48	2.99	3.08	5.03	5.34	6.29	6.45	6.57	6.57
Oman	2.21	3.94	4.31	5.39	5.42	6.28	7.12	7.12	7.37
Pakistan	0.92	1.75	1.90	2.60	2.47	2.95	3.03	3.30	3.39
Qatar	3.67	5.85	6.03	7.33	6.88	7.80	8.09	7.90	7.91
Saudi Arabia	2.29	4.78	5.06	6.10	6.58	6.80	7.04	7.51	7.29
Syria	1.88	3.21	3.54	4.08	4.12	4.47	4.50	4.58	4.66
Tajikistan	1.22	1.64	…	…	…	…	…	…	…
Turkey	2.46	4.24	4.44	5.27	5.01	5.66	5.83	6.00	6.20
Turkmenistan	1.37	1.95	1.89	2.73	2.62	…	…	…	…
United Arab Emirates	4.30	6.78	6.78	6.83	6.73	7.39	7.67	7.94	8.14
Uzbekistan	0.96	1.46	1.75	2.08	2.44	2.78	2.95	4.22	4.53
Yemen	0.85	1.75	1.52	1.93	1.86	2.49	2.66	2.65	2.66
2025 Vision Targeted Countries' Average	2.16	3.55	3.80	4.76	4.83	5.44	5.64	5.84	5.96

4.2. Use Sub-index									
	2002	2007	2008	2010	2011	2012	2013	2015	2016
Iran	0.16	0.61	0.36	0.60	0.85	1.18	1.44	2.19	2.74
Afghanistan	…	…	…	0.13	…	0.20	0.24	0.34	0.47
Armenia	0.07	0.21	0.22	1.41	2.21	2.66	3.02	3.47	3.85
Azerbaijan	0.12	0.61	0.61	1.99	3.07	3.55	4.40	5.66	5.70
Bahrain	0.63	1.97	2.75	2.64	3.92	6.70	7.06	7.54	7.48
Egypt	0.09	0.53	0.68	1.39	2.25	2.55	2.87	2.78	3.14
Georgia	0.05	0.41	0.76	1.31	2.35	2.03	2.58	3.40	4.00
Iraq	…	…	…	…	…	…	…	…	…
Israel	0.79	3.69	4.44	4.65	5.02	5.53	5.53	5.75	6.02
Jordan	0.20	0.75	0.90	1.16	1.55	1.90	2.22	2.44	3.20
Kazakhstan	0.06	0.23	0.60	2.13	3.37	3.73	4.33	4.90	5.15
Kuwait	0.37	1.14	…	4.07	…	…	…	6.03	6.15
Kyrgyz Republic	0.10	0.47	0.54	0.58	…	1.41	1.59	2.00	2.25
Lebanon	0.44	0.89	1.01	1.88	2.37	3.52	4.33	5.46	5.46
Oman	0.24	0.66	0.92	2.18	2.99	3.81	4.65	5.05	5.39
Pakistan	0.09	0.34	0.53	0.29	0.34	0.38	0.42	0.69	1.09
Qatar	0.34	1.46	1.91	4.48	5.70	4.86	5.95	6.03	6.32
Saudi Arabia	0.21	1.10	1.72	2.57	3.28	4.13	4.77	6.03	6.32
Syria	0.07	0.57	0.22	0.72	0.81	0.93	1.07	1.35	1.52
Tajikistan	0.00	0.25	…	…	…	…	…	…	…
Turkey	0.37	1.36	1.59	2.21	2.30	2.98	3.24	3.77	4.18
Turkmenistan	0.01	0.05	0.06	0.07	0.17	…	…	…	…
United Arab Emirates	0.93	2.79	3.87	3.23	3.93	4.90	6.51	6.66	6.82
Uzbekistan	0.04	0.25	0.32	0.81	1.65	1.94	2.09	2.17	2.58
Yemen	0.02	0.05	0.24	0.38	0.52	0.63	0.73	0.99	1.12
2025 Vision Targeted Countries' Average	0.23	0.89	1.15	1.78	2.43	2.83	3.29	3.85	4.13

4.3 Skills Sub-index									
	2002	2007	2008	2010	2011	2012	2013	2015	2016
Iran	5.83	6.32	6.69	6.97	7.30	7.52	7.52	6.96	6.96
Afghanistan	…	…	…	2.74	…	2.98	2.98	2.65	2.65
Armenia	6.98	7.44	7.84	8.23	8.01	8.04	8.04	7.17	7.17
Azerbaijan	6.49	6.78	7.10	7.25	7.28	7.33	7.33	6.47	6.47
Bahrain	7.34	7.14	7.22	7.36	7.47	7.44	7.44	6.50	6.50
Egypt	5.77	6.01	5.83	6.05	5.74	6.33	6.33	5.33	5.33
Georgia	7.39	7.51	7.46	7.16	7.19	7.14	7.14	7.34	7.34
Iraq	…	…	…	…	…	…	…	…	…
Israel	8.20	8.27	8.28	8.71	8.71	8.78	8.78	8.38	8.38
Jordan	7.11	7.17	7.36	7.54	7.35	7.74	7.74	6.68	6.68
Kazakhstan	7.69	8.11	7.95	7.85	8.00	8.06	8.06	7.41	7.41
Kuwait	6.36	6.65	…	7.41	…	…	…	5.59	5.59
Kyrgyz Republic	7.54	7.61	7.87	7.51	…	7.62	7.62	6.96	6.96
Lebanon	6.83	7.36	7.42	7.06	7.68	6.99	6.99	5.46	5.46
Oman	5.72	6.63	6.79	6.93	7.18	6.95	6.95	5.83	5.83
Pakistan	2.44	3.06	3.12	3.19	3.27	3.36	3.36	2.78	2.78
Qatar	6.17	6.64	6.60	6.88	6.92	6.95	6.95	6.03	6.03
Saudi Arabia	5.64	7.04	7.09	7.48	7.60	8.17	8.17	7.30	7.30
Syria	4.53	5.69	5.79	6.07	5.77	6.17	6.17	4.22	4.22
Tajikistan	6.38	6.77	…	…	…	…	…	…	…
Turkey	6.38	6.92	6.96	7.81	7.71	8.34	8.34	7.72	7.72
Turkmenistan	7.03	7.37	6.85	6.87	6.87	…	…	…	…
United Arab Emirates	5.89	6.88	6.88	6.80	7.08	6.79	6.79	5.63	5.63
Uzbekistan	6.77	6.89	6.97	6.96	6.94	6.94	6.94	6.04	6.04
Yemen	3.48	3.79	3.95	3.97	4.04	4.11	4.11	2.54	2.54
2025 Vision Targeted Countries' Average	6.26	6.70	6.76	6.73	6.91	6.85	6.85	5.95	5.95

The data for the ICT Development Index and its respective sub-indexes has been extracted from the following reports:

- "Measuring the Information Society Report 2016." *The International Telecommunication Union (ITU)*. 2016. Web. 1 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2016/MISR2016-w4.pdf>.
- "Measuring the Information Society Report 2015." *The International Telecommunication Union (ITU)*. 2015. Web. 1 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf>.
- "Measuring the Information Society Report 2014." *The International Telecommunication Union (ITU)*. 2014. Web. 1 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf>.
- "Measuring the Information Society 2013." *The International Telecommunication Union (ITU)*. 2013. Web. 1 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013_without_Annex_4.pdf>.
- "Measuring the Information Society 2012." *The International Telecommunication Union (ITU)*. 2012. Web. 1 Mar. 2017. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2012/MIS2012_without_Annex_4.pdf>.
- "Measuring the Information Society 2011." *The International Telecommunication Union (ITU)*. 2011. Web. 1 Mar. 2017. <https://www.itu.int/net/pressoffice/backgrounders/general/pdf/5.pdf>.
- "Measuring the Information Society 2010." *The International Telecommunication Union (ITU)*. 2010. Web. 1 Mar. 2017. <https://www.itu.int/ITU-D/ict/publications/idi/material/2010/MIS_2010_without_annex_4-e.pdf>.
- "Measuring the Information Society 2009: The ICT Development Index." *The International Telecommunication Union (ITU)*. 2009. Web. 1 Mar. 2017. <https://www.itu.int/ITU-D/ict/publications/idi/material/2009/MIS2009_w5.pdf>.