Article

Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran

Marcus Michaelsen

Department of Political Sciences, University of Amsterdam, The Netherlands.
m.michaelsen@uva.nl

Abstract

Transnational information flows and advocacy networks are among the challenges of a globalizing world to which contemporary authoritarian rulers need to adapt. Drawing on research into repressive strategies of the Iranian state against exiled human rights activists and journalists, I show how digital surveillance allows the regime to monitor political activity outside the country and to prepare counter-measures projecting power beyond borders. With the help of digital media, state authorities can expand the scope and scale of potential threats against activists in the diaspora and their ties into the country. I argue that the repressive practices of the Iranian state are not only a response to the transnationalization of political activism but also result of a global securitization of online space. The Iranian case thus demonstrates how contemporary authoritarian power is built and sustained in processes no longer bound to a specific state or territory.

Introduction

Surveillance represents an inherent element of authoritarian rule. Confronted with a “twin problem of uncertainty”, authoritarian power holders can never be fully sure about potential threats to regime stability and their actual success in preventing such threats (Schedler 2013: 21). From the totalitarian dictatorships of the 20th century to today’s “networked authoritarians” (MacKinnon 2011), these regimes have monitored their populations to detect dissent, discern dissatisfaction and preempt challenges. The institutionalized and systematic practices of information gathering under authoritarian rule are not only a means which enables repression and regime preservation but also a distinct form of power and control. The threat of omnipresent security agents collecting up to the most intimate details of individuals’ lives has a chilling effect on the expression of critical opinion, encourages self-censorship and pushes people into conformity (Richards 2013).

How have surveillance practices of authoritarian rulers evolved in the digital age? Current debates on surveillance center on forms of digitized data collection by powerful private and state actors, mostly of Western origin, who operate in increasingly intransparent and transnational settings (Bauman et al. 2014; Lyon 2014). Research on authoritarian surveillance and repression, in turn, tends to be preoccupied with the domestic context (for notable exceptions see: Cooley and Heathershaw 2017; Moss 2016). As a consequence we know little about how authoritarian states use the affordances of digital technologies to extend their influence and control into the transnational realm.

Michaelsen, Marcus. 2017. Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance & Society* 15(3/4): 465-470.

<http://library.queensu.ca/ojs/index.php/surveillance-and-society/index> | ISSN: 1477-7487

© The author(s), 2017 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

Authoritarian regimes have never been as isolated as their determination to control borders and ideas made believe. But today they are ever more closely tied into an international environment that shapes their incentives and capacities (Glasius 2015; Tansey 2016). Transnational information flows and advocacy networks count among the challenges of a globalizing world to which these rulers need to adapt. Digital media have helped activists and journalists to undermine authoritarian information controls, expose rights violations and tarnish the public image regimes seek to present to domestic and international audiences (Keck and Sikkink 1998; Tarrow 2005). In response to the increasing role that online media and social networks play for political activism and the circulation of news and opinion, authoritarian states have built sophisticated systems of internet control. From initial defensive methods, like content blocking and filtering, they have shifted to more offensive approaches, using disinformation, cyberattacks, online harassment and surveillance to suppress critical voices on the internet (Deibert 2013; Gunitsky 2015; Pearce 2015). These measures are not only directed against domestic activists but target also opponents outside the country.

Drawing on research into the repressive strategies of Iranian state actors against exiled human rights activists and journalists, I show in this contribution how digital communication surveillance enables the regime to project power beyond borders.¹ Iran's security agencies rely on low-scale technical expertise and human information gathering to monitor political activity outside the country's territorial jurisdiction and to prepare retaliatory or preemptive counter-measures. Not all measures in this repressive tool-kit are new but digital surveillance expands the scope and scale of potential threats against transnational activists and their networks. It is facilitated by the increasing penetration of everyday life by the internet and social media, leading to a convergence of different social roles and activities on online platforms. As the communication structures of transnational advocacy networks rely heavily on digital media, they produce an array of information that regimes can exploit for purposes of extraterritorial state control (Fuchs and Trottier 2015; Hankey and Ó Clunaigh 2013).

The Case of Iran

Iran's Islamic Republic emerged out of the revolutionary turmoil in 1979 and consolidated during the war against Iraq. Although the political system allows for a limited state-managed political competition and regular elections that clearly affect the country's direction, repression remains one of its defining features. The regime is openly authoritarian in the constraints it imposes on civil liberties, political dissent and cultural expression. A reactionary backlash against attempts to reform the political system at the end of the 1990s strengthened the clout of the security establishment and most notably the Revolutionary Guards, a branch of the military constitutionally mandated to protect "the revolution and its achievements" (Brumberg and Farhi 2016: 2). The hard-liners' rise culminated in the contested re-election of President Mahmoud Ahmadinejad in 2009 when the regime violently crushed opposition protests claiming election fraud. As the arena for political and civic activism narrowed, hundreds of activists and opposition supporters ended up in prison or left into exile. Despite the election of a moderate president in 2013, the influence of Iran's 'deep state' persists, with security agencies often operating in parallel, at times in competition to the government (Ansari 2010; Human Rights Watch 2012; Iran Human Rights Documentation Center 2010).

¹ For this research project, the author conducted 15 semi-structured qualitative interviews of 1-2 hours with Iranian human rights activists and journalists based in seven different countries in Europe and North America. All respondents left Iran after the controversial elections of 2009 and were identified through an existing network of contacts and further introductions ('snowballing'). They included high profile human rights defenders, such as Nobel Laureate Shirin Ebadi, as well as lesser known figures. Additional interviews were held with two external experts on Iranian cyberattacks against civil society and two program managers of Persian language news media in Europe. In addition, the author participated in a digital security training for Iranian civil society activists from Iran (organized outside the country) as well as several events dedicated to internet controls and digital security in Iran.

Digital media played an important role for the protest movement of 2009, fostering internal debate as much as raising international awareness (Michaelsen 2015). In response, the regime enhanced its capacities for internet control. Authorities started blocking websites and arresting critical bloggers already in the early 2000s but with the evolvement of circumvention and anonymization tools resorted to more aggressive measures, including deep packet inspection, hacking of opposition media, and targeted surveillance (OpenNet Initiative 2013). While their actual technical capabilities remain obscure, security agencies rely on the chilling effect of mediatized surveillance operations. Now and then, state television airs forced confessions of arrested social media users to highlight the regime's skills in cyber-policing. In addition to internet activists and journalists, these campaigns also target other online communities who are considered to transgress official norms. In 2014, for instance, six young Iranians were detained for circulating a home-made music video with an interpretation of Pharrell Williams' song "Happy" (Kamali Dehgan 2014). In 2015, the cybercrime unit of the Revolutionary Guards announced that it was monitoring the Facebook activities of Iranians on a large scale and had arrested groups of social media users for promoting "obscene content, western-inspired lifestyles and anti-religious jokes" (Center for Human Rights in Iran 2015).

Yet the capabilities of the Iranian state for internet control and surveillance result not only from the determination to contain domestic dissent. They have also developed in line with the global securitization of online space. Iran was a target of one of the first international cyberattacks against critical state infrastructure. As later disclosed by the Snowden files, the U.S. government's infiltration of sophisticated computer viruses into the Iranian nuclear facilities may have given Iran an opportunity to learn from the deployed techniques (Greenwald 2015). The Iranian regime's view of the internet as a tool of Western aggression was also confirmed by U.S. State Secretary Hillary Clinton's speeches on internet freedom pledging support to internet activists worldwide (Council on Foreign Relations 2010). Moreover, despite international sanctions, Iran finds access to the global market for surveillance technology and has made use of web monitoring devices manufactured by Western companies (Citizen Lab 2013). Finally, knowledge and technology for internet controls are also exchanged among authoritarian countries, as evidenced by Iran's cooperation with China (Stecklow 2012).

Given these external stimuli, it is evident that Iranian security agencies also put the acquired capabilities to use in an international context. Based on inferences from malware code, infrastructure and target selection, a range of cyberattacks in countries of the Middle East, Europe and North America has been attributed to Iranian state or state-sponsored actors. Iranian exiles and diaspora organizations figure prominently among the targets (Guarnieri and Anderson 2016). Online espionage and malware spearphishing are part of a broader arsenal of repressive tactics directed against human rights defenders and journalists outside the country. Digital approaches are often combined with more traditional measures, such as pressure on relatives in the country and slander in state media. State authorities seek to compromise the ties of exiled activists into the country and to disable their 'voice': the ability to provide domestic and international audiences with information that contravenes regime discourse. For this reason, they particularly target outspoken public figures among the exile community as well as journalists working for Persian programs of foreign media institutions, such as the BBC and Voice of America (VoA) (Michaelsen 2016). Surveillance is fundamental to all these measures of transnational repression as it allows state agents to identify their targets and to develop responses in accordance to the challenge they perceive.

State Agents Reaching Beyond Borders

In a series of intrusion attempts against social media and email accounts of activists in the diaspora, Iranian agents used information gathered online to coax their targets into opening malware files. Activists received invitations to seminars in their field of expertise and journalists press releases from opposition figures. Other diaspora members even received notices about the expiry of their residence permits by fake emails from immigration services (Guarnieri and Anderson 2016). Combining phone calls, SMS-messages and phishing emails, attackers also tried to break the so-called two-factor verification, an additional security barrier of email providers (Citizen Lab 2015). Reza², an Iranian cybersecurity expert, reports that he was contacted over the phone and by email from someone seeking advice to prepare a tournament of his favorite sport in Iran and who tried to convince him to open a compromised file. He emphasizes: *“When I was analyzing it, I realized that there must be a number of people behind it, quite scary. Not for the technical sophistication but in terms of social engineering and human effort it’s mind-blowing”* (Interview, 26 August 2015).

The US-based journalist Negar Mortazavi, who experienced several attempts to penetrate her email and social media accounts, underlines that agents aim to gather more information on diaspora activities: *“They are very interested in discovering and breaking into networks. [...] It is about who you are talking to and connecting with to mobilize for a campaign.”* (Interview, 30 October 2015). Compromised accounts are then often used for further information theft and threats. Soon after a Revolutionary Guards unit arrested Arash Zad, an Iranian start-up entrepreneur traveling from Tehran airport in August 2015, many of his contacts inside and outside the country received phishing emails from his account (Alimardani 2015). The outspoken journalist Masih Alinejad, who runs campaigns for political prisoners and women’s rights, reports that agents used the hacked Facebook profile of a relative to reach out to her teenage son living with her in New York (Interview, 16 September 2015). Nader*, an Iranian civil society activist now residing in Europe, points out that surveillance precedes all other threats and must be seen as a means of control: *“Every time we give an interview or are doing something more publicly, there is a response from the other side, for instance from [hardline newspaper] Keyhan. Also, the attempts to hack emails clearly give a signal that observation is taking place”* (Interview, 30 September 2015).

Journalists working for Persian programs of foreign news media reaching out to audiences inside Iran receive particular attention from Iranian security agencies. By monitoring their work, state agents seek to uncover and cut any links into the country, points out Ali Fotovvati, journalist for a Europe-based Iranian news website and online radio: *“They are closely watching us. I have talked to friends who were interrogated in Iran and they were asked about our staff members. Some of our contributors write under a pseudonym and in the interrogations, authorities try to find out who is behind that name”* (Interview, 6 October 2015). Vahid Pourostad, a journalist with Radio Farda, the Persian program of Radio Free Europe in Prague, emphasizes that the systematic collection of media content is used to prevent outside media from accessing sources and threaten contributors in the country: *“All our reporting is documented, transcribed and given to the responsible authorities. [...] In the interrogations they confront people with the recordings”* (Interview, 16 November 2015).

Considering the risks that people in Iran encounter when collaborating with outside activists, digital surveillance represents a clear threat to the dynamics of transnational exchange fostered by the internet and social media. Transnational activists need to invest additional effort and resources in the protection of their contacts and communications. In consequence, digital security has become an important aspect of civic and political activism, as journalist Negar Mortazavi explains: *“I always have this fear that maybe there is a new method that I don’t know about, that I am not paying attention to. Then, there is also the fear that the other side is not secure [...] Cybersecurity is not my field and I am not even interested in it. But it’s something that I have to follow just to be safe”* (Interview, 30 October 2015). In a spiral of mutual influence,

² Name of interviewee changed.

surveillance casts a particularly menacing shadow over the resistance it raises: Workshops and trainings dedicated to digital security and information freedom in Iran need to be held under precautions, especially when they include participants from inside Iran, in order to prevent the interception of logistic communications or traces of the event on social media. Although the threat of surveillance does not deter the activists interviewed for this research, it puts their contacts into the country at risk. In this sense, surveillance is not only a means enabling further repression, but it serves a direct tactic of control, hindering the outreach and effects of transnational activism.

Conclusion: Globalized Authoritarian Practices

The Iranian example shows how surveillance of digital communications allows authoritarian state actors to expand their power beyond borders. Responding to activities of exiled dissidents, journalists and human rights defenders, state agents seek to control transnational forms of information circulation, political expression and association. They aim to gather information that helps them to prepare additional tactics of repression and to introduce mistrust and fear into communication networks. Their intentions thus correspond to the traditional aims of surveillance under authoritarian rule. With the help of digital media, however, these practices reach beyond state boundaries to target individuals dispersed across a number of countries. Because of the internet's increasing centrality for professional and private activities as well as the rapid evolvement of digital surveillance technologies and methods, the potential impact of surveillance has gained a new quality. The threat of targeted information collection through email intrusions and social media hacking enables state authorities to maintain a latent pressure over activists, even if they are no longer residing in the country. Moreover, they can react quickly to any activity perceived as a threat to authoritarian information controls.

The surveillance practices of the Iranian regime show how contemporary authoritarian power is built and sustained in processes that are no longer bound to a specific territory or state entity. The incentives and intentions behind these practices are globalized in a double sense: on the one hand, with the extension of digital surveillance beyond the borders of the nation-state authoritarian power holders respond to the challenges of transnational advocacy and information activism. On the other hand, the deployed tools and techniques develop in par with a "globalization of security and surveillance" (Murakami Wood 2012: 333), underlining that in even in 'classical' and ostensibly isolated authoritarian regimes surveillance and control are produced and re-produced in global bonds and exchange.

Acknowledgments

Research for this publication has been conducted within the "Authoritarianism in a Global Age" project at the University of Amsterdam, funded by the European Union's Horizon 2020 research and innovation program. An earlier version was presented at the "Telecommunication Politics in Authoritarian Contexts" workshop in May 2017 at the University St. Gallen, where I benefitted from the comments of participants. I would also like to thank the anonymous reviewer for constructive comments.

References

- Alimardani, Mahsa. 2015. "The Arrest of Arash Zad, Iran's Start-Up Kid". *Global Voices Advocacy*, September 23. Accessed June 13, 2017. <https://advox.globalvoices.org/2015/09/23/the-arrest-of-arash-zad-irans-start-up-kid>.
- Ansari, Ali M. 2010. *Crisis of Authority: Iran's 2009 Presidential Elections*. London: Royal Institute of International Affairs.
- Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and Rob Walker. 2014. "After Snowden: Rethinking the Impact of Surveillance". *International Political Sociology* 8 (2): 121-44.
- Brumberg, Daniel, and Farideh Farhi (editors). 2016. *Power and Change in Iran. Politics of Contention and Conciliation*. Bloomington, IN: Indiana University Press.
- Center for Human Rights in Iran. 2015. *Facebook Users Arrested, Others Will Be Arrested Soon, IRGC States*, March 13. Accessed June 13, 2017. <https://www.iranhumanrights.org/2015/03/facebook-users-arrested>.

- Citizen Lab. 2013. *Some Devices Wander by Mistake: Planet Blue Coat Redux*. Accessed June 13, 2017. <https://citizenlab.org/2013/07/planet-blue-coat-redux>.
- Citizen Lab. 2015. *London Calling: Two-Factor Authentication Phishing from Iran*. Accessed June 13, 2017. <https://citizenlab.org/2015/08/iran-two-factor-phishing>.
- Cooley, Alexander A., and John Heathershaw. 2017. *Dictators Without Borders: Power and Money in Central Asia*. New Haven, CT: Yale University Press.
- Council on Foreign Relations. 2010. *Clinton's Speech on Internet Freedom*. Accessed June 13, 2017. <http://www.cfr.org/internet-policy/clintons-speech-internet-freedom-january-2010/p21253>.
- Deibert, R. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart.
- Fuchs, Christian, and Daniel Trottier. 2015. "Towards a Theoretical Model of Social Media Surveillance in Contemporary Society". *Communications* 40 (1): 113-135.
- Glasius, Marlies. 2015. "Reconceptualizing Authoritarianism". *APSA Comparative Democratization* 13 (2). Accessed June 13, 2017. <http://live-apsa-cd.pantheonsite.io/wp-content/uploads/2015/07/APSA-CD-June-2015.pdf>.
- Greenwald, Glenn. 2015. "NSA claims Iran learned from Western cyberattacks". *The Intercept*, February 10. Accessed June 13, 2017. <https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks>.
- Guarnieri, C., and C. Anderson. 2016. *Iran and the Soft War for Internet Dominance*. Working Paper. Accessed June 13, 2017. <https://iranthreats.github.io/us-16-Guarnieri-Anderson-Iran-And-The-Soft-War-For-Internet-Dominance-paper.pdf>.
- Gunitsky, Seva. 2015. "Corrupting the Cyber-commons: Social media as a Tool of Autocratic Stability". *Perspectives on Politics* 13 (1): 42-54.
- Hankey, Stephanie, and Daniel Ó. Clunaigh. 2013. "Rethinking Risks and Security of Human Rights Defenders in the Digital Age". *Journal of Human Rights Practice* 5 (3): 535-47.
- Human Rights Watch. 2012. *Why They Left. Stories of Iranian Activists in Exile*. Accessed June 13, 2017. https://www.hrw.org/sites/default/files/reports/iran1212webwcover_0_0.pdf.
- Iran Human Rights Documentation Center. 2010. *Violent Aftermath: The 2009 Election and Repression of Dissent in Iran*. Accessed June 13, 2017. <http://www.iranhrdc.org/english/publications/reports/3161-violent-aftermath-the-2009-election-and-suppression-of-dissent-in-iran.html>.
- Kamali Dehgan, Saeed. 2014. "Iranian Pharrell Williams fans detained over 'obnoxious' video". *The Guardian*, May 20. Accessed June 13, 2017. <https://www.theguardian.com/world/2014/may/20/iranian-pharrell-fans-in-custody-after-making-happy-video>.
- Keck, Margaret E., and Kathryn Sikkink. 1998. *Activists Beyond Borders. Advocacy Networks in International Politics*. New York: Cornell University Press.
- Lyon, David. 2014. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique". *Big Data & Society* 1 (2). doi: 10.1177/2053951714541861.
- MacKinnon, Rebecca. 2011. "China's Networked Authoritarianism". *Journal of Democracy* 22 (2): 32-46.
- Michaelsen, Marcus. 2015. "Beyond the 'Twitter-Revolution': Internet and Political Change in Iran". In *Global Activism. Art and Conflict in the 21st Century*, edited by Peter Weibel, 384-395. Cambridge, MA: MIT Press.
- Michaelsen, Marcus. 2016. "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State". *Globalizations*. doi: 10.1080/14747731.2016.1263078.
- Moss, M. D. 2016. "Transnational Repression, Diaspora Mobilization, and the Case of the Arab Spring". *Social Problems* 63: 480-498.
- Murakami Wood, David. 2012. "Globalization and Surveillance". In: *Routledge Handbook of Surveillance Studies*, edited by Kirstie S. Ball, Kevin D. Haggerty, and David Lyon. New York: Routledge.
- OpenNet Initiative. 2013. *After the Green Movement: Internet Controls in Iran 2009-2012*. Accessed June 13, 2017. www.opennet.net/iranreport2013.
- Pearce, Katy E. 2015. "Democratizing kompromat: The Affordances of Social Media for State-sponsored Harassment". *Information, Communication & Society* 18 (10): 1158-74.
- Richards, Neil M. 2013. "The Dangers of Surveillance". *Harvard Law Review* 126 (7): 1934-65.
- Schedler, Andreas. 2013. *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. Oxford: Oxford University Press.
- Stecklow, Steve. 2012. "Chinese firm helps Iran spy on citizens". *Reuters*, March 22. Accessed June 13, 2017. <http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322>.
- Tansey, Oisín. 2016. *International Dimensions of Authoritarian Rule*. Oxford: Oxford University Press.
- Tarrow, Sidney. 2005. *The New Transnational Activism*. New York: Cambridge University Press.