Transforming Threats to Power: The International Politics of Authoritarian Internet Control in Iran

MARCUS MICHAELSEN[1]
University of Amsterdam, The Netherlands

Authoritarian Internet control is generally explained by domestic power preservation: to curtail dissent within their borders, authoritarian regimes censor, monitor, and shape online communications. Yet this focus neglects important external factors. As a global communication technology, the Internet carries strategic and normative interests of competing international actors. This article investigates the influence of international politics on practices of Internet surveillance and censorship. Using the case of Iran, I analyze how opposition to the West, and particularly to the United States, led the Iranian state to perceive the Internet as a strategic battleground for regime stability. I argue that external threats in the form of democracy promotion, cyberattacks, and sanctions have created conditions enabling the Iranian state to advance and justify capabilities for censorship and surveillance. They have also pushed the regime to build a "national Internet" that is more resistant to outside influence and open to state control. Authoritarian practices are thus produced in international struggles over the use, content, and infrastructure of digital technologies.

Keywords: information and communication technologies, censorship, surveillance, authoritarianism, international relations, Iran

The fundamental aim of authoritarian rulers is to maintain and expand political power. In the field of Internet politics, authoritarian power holders have pursued this aim by establishing sophisticated systems of Internet control to curb alternative information and dissent perceived as challenge to their rule. They have also come to benefit from digital communication technologies for information manipulation, monitoring, and surveillance. A growing body of research sheds light on these restrictive and offensive strategies of authoritarian state control over the Internet. It explains evolving Internet controls primarily by regime reactions to domestic forms of dissent, protest, and political mobilization enabled by digital media. Yet this focus, important as it is, tells only half of the story because it neglects external factors shaping the decisions and capacities of authoritarian power holders. Contemporary authoritarian regimes are embedded in an international environment that influences their political considerations and opportunities (Glasius, 2018; Tansey, 2016). They are able to draw political capital from their position and struggles in the international

Marcus Michaelsen: m.michaelsen@uva.nl
Date submitted: 2017–12–07

[1] This research was supported by the Authoritarianism in a Global Age project at the University of Amsterdam and received funding from the *European Research Council (FP7/2007-2013)/ERC grant agreement number 323899.*

system to consolidate power (Ehteshami et al., 2013). As a global communication structure transcending geographical and political borders, the Internet is inevitably linked to questions of international relations and politics. The way authoritarian regimes perceive the Internet's risks and benefits and how they develop and use it, depends on their collaboration, competition, and conflict with other states. These outside influences need to be taken into account to develop a complete picture of how authoritarian practices of Internet control emerge and take shape.

Due to the preoccupation with domestic dynamics, much of the literature on digital technologies in authoritarian contexts still seems entangled in a debate on whether the Internet is "empowering activists or autocrats" (Rød & Weidmann, 2015). This focus not only ignores international politics but also suffers from problematic conceptualizations of technology. The Internet is taken as a given variable unfolding its impact: either as a neutral tool, its effects depending on how and by whom it is put to use, or as a carrier of specific purposes deciding its social and political consequences. Especially the latter view has led to a stylized debate portraying the Internet as a "liberation" or "repression technology" (Diamond, 2010; Morozov, 2011). Deterministic approaches to technology, however, underestimate the extent to which its development is shaped by competing interests and ideas of different social actors. Technology design, expansion, and regulation are an expression of underlying power relations and contestation over its form and use (Pinch & Bijker, 1984). Shifting the focus from the impact of the Internet to the politics that surround it allows a deeper understanding of how it relates to authoritarian power.

Addressing these two shortcomings in the literature, this article investigates how the capability and motivation of authoritarian regimes to engage in practices of Internet control are shaped by international politics. Using the case of Iran, I show how geopolitical and ideological opposition to the West, particularly to the United States, led the Iranian regime to perceive the Internet as a strategic battleground for regime stability and to strengthen its hold over critical Internet infrastructure. I argue that external threats in the form of democracy promotion, cyberattacks, and sanctions have created conditions enabling the Iranian state to advance and justify capabilities for censorship and surveillance. These threats have also pushed the regime further in its attempts to build a national information network that is more resistant to outside influence and open to state control. Therefore, it is not only the desire to thwart domestic opponents and dissent but also the response to international challenges that brings the regime to engage in "digital illiberal and authoritarian practices"—infringements on individual privacy and violations of freedom of expression (Glasius & Michaelsen, this Special Section).

The article begins with a discussion linking research on authoritarian Internet controls with studies on the international dimensions of authoritarian rule. Both literatures fail to grasp the influence of international politics on the decisions and capacities of authoritarian regimes controlling the Internet to consolidate their power. Only scholarship at the intersection of international relations and science and technology studies helps to highlight that the adoption and development of digital technologies are indeed tied into international power struggles between political actors with competing strategic and normative interests. Turning to the case of Iran, I explore how external threats in the form of Internet freedom promotion, cyberattacks, and international sanctions have shaped the motivation and capacity of the Iranian regime to engage in practices of Internet control. The examination of Iran's national Internet finally underlines how the Iranian state's desire to control domestic dissent *and* to resist foreign interference in digital communication networks has been translated into a major project of altering Internet infrastructure in accordance with political interests and ideas.

The article builds on a single-country case and an exploratory approach to allow for deep contextualization and comprehensive analysis. Although the aim is not to reach generalizable conclusions, the outlined findings and arguments can relate to other countries and serve as a point of departure for further, possibly comparative, research. I rely on media and advocacy reports on Iranian Internet governance and regulation as well as official documents and interviews with experts and activists dealing with Iranian Internet policies.

The Politics of Internet Control

Authoritarian Internet controls are considered to have grown in different "generations" as states responded to the evolvement of technologies and challenging forms of usage (Deibert, Palfrey, Rohozinski, & Zittrain, 2011). Popular protests fanned by social media, particularly during the Arab Spring uprisings, are among the factors that seem to have pushed many authoritarian states to improve their capabilities for monitoring and disrupting online communication (Hussain & Howard, 2013; Koesel & Bunce, 2013). In parallel, regimes learned to use digital technologies to shape public opinion, mobilize supporters, and track emerging grievances, thus updating legitimation strategies and administrative performance (Goebel, 2013; Gunitsky, 2015; MacKinnon, 2011; Morozov, 2011). Although this scholarship demonstrates that authoritarian rulers can successfully incorporate digital technologies into their repertoires of repression and legitimation, it focuses predominantly on domestic strategies of power preservation. Containing information flows and dissent within borders certainly represents a central motive for authoritarian regimes, but, as outlined in the conceptual prologue to this Special Section, practices of surveillance and information control are also produced and diffused in configurations of transnational and interstate actors (Glasius & Michaelsen, this Special Section).

Research on Internet governance and cybersecurity notes how the transposition of conventional geopolitics into cyberspace pushes many states to assert greater authority over the Internet (DeNardis, 2014; Segal, 2016). As cyberattacks, espionage, and disinformation campaigns play a greater role in international politics, states, both democratic and authoritarian, upgrade their offensive cyber-capabilities (Buchanan, 2016). Deibert and Crete-Nishihata (2012) argue that the securitization of cyberspace supports norms and principles that are more permissive toward surveillance and content controls. After the dominant position of the United States in global Internet governance has been weakened in consequence of the Snowden revelations, contesting powers such as China and Russia promote ideas of "Internet sovereignty" and "information security," opting for more state control over global information flows (Ebert & Maurer, 2013; see also Kerr, McKune, & Ahmad, this Special Section). Such international dynamics need to be explored more systematically in terms of their potential to stimulate and enable authoritarian practices of Internet control.

With a focus on state-society relations and the effects of the Internet on either side, current research on digital technologies in authoritarian contexts has largely ignored the influence of international politics on the decisions and capabilities of regimes seeking to control the Internet. In addition, research interests are often grounded in presupposed technical qualities of the Internet. On the one hand, the networked and flexible character of digital communications is presented as a challenge to power holders seeking to control information flows. On the other hand, the possibilities to monitor users, collect data, and shape public opinion are seen as qualities of the Internet that support the exercise of authoritarian power. According to Carr (2016), this approach has brought about an "empirical stalemate," because the Internet in fact "both enhances and undermines state power in complex and important ways but it does so, at least in part, as a consequence of decisions by politicians" (p. 31). To understand how political decisions about the Internet take shape and what political interests they represent, it is necessary to unpack the politics of technology. Technology is neither a neutral tool nor following a determined path of development; rather, it is "an *expression* of the norms, values and expectations of society" (Carr, 2016, p. 18, italics in the original). Technology develops in a specific social and historical context influenced by competing visions of social actors over its form and purpose. In this sense, "the ability to design technological objects is understood as a unique form of power" (McCarthy, 2015, p. 33). In international relations, the innovation, adoption, and expansion of technology can be seen as a field of power struggles between international actors who pursue diverging strategic interests and norms definitions (McCarthy, 2017).

Given the U.S. government's central role in the development and expansion of the Internet, McCarthy (2015) argues that the network's current configuration embodies key interests of U.S. foreign and economic policy, "centered on opening markets and liberalizing other states" (p. 153). States opposing the political values that motivate the idea of a "free flow of information" and are embedded in the Internet's infrastructure need to mobilize power and resources to change the technology according to their own interests (McCarthy, 2015, p. 93). Two speeches by U.S. secretary of state Hillary Clinton, in 2010 and 2011, exemplify this intertwining of technology development and foreign policy: At a time when Middle Eastern regimes tumbled as a result of protest movements visibly mobilizing through digital media, Clinton pledged support to tech activists fighting Internet censorship. This discourse not only exerts "symbolic pressure upon authoritarian governments" (McCarthy 2015, p. 103) but also forces them to respond to any policy measures that flow from it.

Adopting a perspective that emphasizes the social construction of technology helps us understand why the practices and policies of authoritarian states trying to control the Internet cannot be explained by strategies of domestic power preservation alone. As a global information structure, the Internet embodies international power relations, with competing actors trying to shape and use technology according to their norms and interests. For authoritarian states seeking to maintain and expand their political power, this technopolitical environment creates impulses and opportunities for developing and justifying digital authoritarian practices.

International Dimensions of Authoritarian Rule

International relations and linkages to other states play an important role for strengthening or weakening authoritarian regimes (Levitsky & Way, 2010; Tansey, 2016). Regimes can translate their position and struggles in the international system into strategies of legitimation and repression, ensuring compliance with and support for their rule. The international environment also offers opportunities for transferring practices and resources of power consolidation.

International sanctions are among the harshest measures foreign actors employ to coerce an authoritarian regime into policy changes. Yet they often fail to have the desired effect, because "sanctions create conditions that help consolidate the regime's hold on power and create new incentives . . . to limit democratic freedoms" (Peksen & Drury, 2010, p. 247). Regimes perceive external pressure as a threat to their survival and to state sovereignty, to which they respond by intensifying internal repression and tightening the ranks of the ruling elite. Sanctions can also promote nationalist and other "defensive" legitimation strategies or push the regime to enhanced cooperation with other authoritarians (Hoffmann, 2015; Wood, 2008). Sanctions targeting resources and capacities for Internet censorship may have similar adverse effects, even though they do not threaten the very existence of a regime. Constrained access to Western technology and software, for instance, can further the development of domestic alternatives and infrastructures more open to state interference. Acting as authoritarian sponsors, countries such as Russia and China can provide technical expertise and discursive legitimation for stronger state control over digital communication technologies (Kerr, McKune, & Ahmad, this Special Section).

In addition to sanctions, Western democracy promotion represents another external challenge provoking authoritarian persistence. The color revolutions, for instance, went along with extensive Western support for civil society, which led regimes to tighten the rules for nongovernmental organizations and external aid (Finkel & Brudny, 2012). With the increasing attention to the role of digital media for civil society and human rights activism, funding for Internet activists and anticensorship measures has become a central component of Western democracy promotion (Christensen, 2011; Hussain, 2014). Although activists have voiced concern about a potential backlash against such programs, there is scarce knowledge on how support for Internet freedom and activism shapes authoritarian rulers' decision making on Internet controls (Gharbia, 2010).

The international environment not only creates threats that resilient authoritarian rulers can translate into strategies of power maintenance but also opens up opportunities for learning and diffusing policies, practices, and discourse from one state to another (Ambrosio, 2010). Authoritarian learning occurs not only between authoritarian regimes but whenever there is an adoption of "non-democratic strategies that autocrats use to secure their rule, and once in power, to fend off challenges and ensure regime revival" (Tansey, 2016, p. 55). Yet learning processes among authoritarian counterparts still form the core interest of this research approach, although authoritarian practices could also be adopted by or transmitted from democratic regimes or transnational and private actors (Hall & Ambrosio, 2017, p. 154). Even less attention has been given to the possible diffusion or stimulation of authoritarian practices in international competition and conflict. As the case study of Iran in this article demonstrates, such dynamics of "learning from adversaries" clearly merit further attention. In addition, research on authoritarian diffusion and learning has shown scarce interest in Internet control. Examinations of learning mechanisms during the Arab uprisings, for instance, focus on different strategies of regime survival but neglect responses to digital media—despite the prominent role that online networks played for the cascading of protest patterns (Bank & Edel, 2015; Josua & Edel, 2015; Koesel & Bunce, 2013).

Although the scholarship on international dimensions of authoritarian rule highlights important mechanisms allowing authoritarian regimes to capitalize on outside influences, it largely ignores digital technologies. As outlined above, the Internet as a global communication system ties into the dynamics of international politics, because its infrastructure and usage are shaped by the interests and ideas of international actors. Therefore, the decisions of authoritarian states on how to govern digital technologies as part of their power strategies cannot be divorced from their position and struggles in the international system. To better grasp the exercise and resilience of authoritarian power in the digital age, it is necessary to understand how external factors such as authoritarian diffusion and learning or sanctions, democracy promotion, and other threats to strategic interests influence a regime's inclination and capacity to engage in practices of Internet control.

This article uses the case of Iran to explore how international politics shaped state control over the Internet. Iran's foreign relations are informed by a worldview emphasizing distrust of foreign interference and a desire for autonomy and independence. Antagonism to the West, and particularly to the United States, is one of the ideological pillars of the regime. Domestic dissent is frequently framed as foreign intervention, stigmatizing advocates of political change as outsiders. But resistance against U.S. hegemony has also helped Iran build relations among other non-Western powers. The regime is thus able to exploit its international position for strategies of legitimation and coercion (Warnaar, 2013). The following discussion explains how Iran's perception of and responses to Western promotion of Internet freedom, cyberattacks, and sanctions contributed to the motivation and capability of the state to resort to digital illiberal and authoritarian practices and to justify the building of a state-controlled national Internet.

Internet and Politics in Iran

From the early days of its expansion in Iran, the Internet played a critical role for political debate and information exchange. Due to the restrictions for print and broadcasting media, websites and blogs quickly became popular channels for news and discussion. From the mid-2000s, the factional conflicts of Iran's fragmented political elite played out online. During the 2009 protests against the results of the presidential elections, digital media were decisive for the internal communication and the international perception of the opposition Green movement (Michaelsen, 2015; Rahimi, 2011).

The Iranian state, in turn, has gradually increased its control over the Internet, starting from first website blockings in 2003. Since then, the censorship regime has become more technically sophisticated, comprehensive, and centralized. Technical restrictions are complemented by a legislative framework, punishing "attempts against national security" and "the undermining of moral values" (Article 19, 2013). Different sections in the country's vast security apparatus monitor and repress critical online activity (OpenNet Initiative, 2013). But the Iranian government sees the Internet also as an opportunity for development and economic progress. Acknowledging the importance of information technologies, the building of communication infrastructure is part of the so-called five-year plans that guide the development of the country. Under current president Hassan Rohani, the number of Internet users has reached 53% of the population. Growth has been particularly impressive in terms of mobile Internet, which reached 47 million users in 2017 (Mehr News, 2017).

Examinations of Iran's evolving censorship regime typically focus on domestic dynamics in line with the general research on authoritarian Internet controls. The overall ambition of the regime to contain dissent and alternative cultural expression is considered a principle driver of state control over the Internet. The challenge of the 2009 protests further accentuated the state's desire to monitor and suppress critical online activity (OpenNet Initiative, 2013). These explanations certainly cover central motives, but they leave out international factors shaping the digital illiberal and authoritarian practices of the Iranian state. As described in the next section, the Iranian regime's policies and practices are also formulated around its responses to perceived ideological and material threats from the West, particularly from the United States.

Responding to Democracy Promotion and the Internet Freedom Agenda

The perception of media as channels of foreign influence presents a prominent notion in the ideology of the Iranian regime. In the 1990s, satellite television was denounced as a vehicle of the "Western cultural invasion"—a view harking back to prerevolutionary ideas about the dangers of Westernization and foreign meddling in Iran (Kian, 1995). In the same vein, the regime considered the Internet an instrument in the "soft war" that the West, particularly the United States, waged against the Islamic Republic by undermining moral values and stirring discontent in Iran (Price, 2012). Supreme Leader Ali Khamenei, in his speeches, described digital media as "tools of cultural infiltration and domination" that "lure away our youth from religion and holy beliefs" (Khamenei, 2016, para. 28; 2017, para. 18).

The discourse on soft war was a direct response to the notion of soft power undergirding efforts of U.S. democracy promotion, which the regime perceived as a threat (Sreberny, 2013). In February 2006, U.S. Congress authorized funds for public diplomacy, aid to civil society, and media programs targeting Iran. In return, Iranian state authorities put pressure on journalists, academics, activists, and everyone else who might have been connected to the democracy fund (Azimi, 2007; Tezcür, 2012). Persian-language programs of external media such as the BBC, Voice of America, and Radio Free Europe, aimed at audiences in Iran via satellite and online media, were met with particular suspicion, and in-country contributors were persecuted. In spring 2009, the Revolutionary Guards' Centre for Organized Cybercrime announced that it had uncovered several subversive groups who used the Internet to agitate against the Islamic Republic and were supported by foreign powers (BBC Persian, 2009). During the 2009 election crisis, such threat scenarios were reinforced by news that the U.S. administration contacted Twitter at the height of the protests to ask for a delay of a planned maintenance in order to maintain access for Iranians who were using the social networking service to communicate during the demonstrations (Pleming, 2009). In the show trials against prominent reformists in summer 2009, the prosecutor explicitly mentioned Facebook and YouTube as tools of U.S. psychological warfare and manipulation (Iran Human Rights Documentation Center 2010, p. 76).

When Western governments intensified the promotion of Internet freedom in the immediate aftermath of Iran's election crisis and the Arab uprisings, the Iranian regime could see these initiatives only as a continued external confrontation through communication technologies. With the wave of protests in the Middle East, fueled and publicized by social media, the interest of Western governments in the Internet as a tool for democratic change surged. Summits and initiatives on Internet freedom brought together policy makers and donor organizations, technology companies and activists. Significant funds were poured into circumvention software and other projects countering Internet censorship. The politics of technology development and control suddenly figured prominently on the political agenda (Christensen, 2011; Hussain, 2014).

The United States was clearly leading the initiative for Internet freedom. In a widely discussed speech in January 2010, U.S. secretary of state Hillary Clinton (2010) linked Internet freedom to a fundamental battle against dictatorship and criticized practices of Internet control as "a new information curtain [that] is descending across much of the world" (para. 17). Clinton warned that "nations that censor the Internet should understand that our government is committed to helping promote Internet freedom" (para. 39). Six months after Iran's election protests had for the first time pushed the notion of a social media revolution onto the front pages of Western media, Clinton referred explicitly to the events in Iran, criticizing government "brutality" and "intimidation" and hailing the courage of citizen journalists and ordinary Iranians speaking out on the Internet. In his address to the Iranian people on the occasion of the Persian New Year, in March 2012, President Obama also criticized "the electronic curtain . . . around Iran" that prevents "the free flow of information and ideas into the country" (Pitney, 2012). In line with this vision, the State Department established the Internet Freedom Program to "counter the efforts of authoritarian regimes to censor, monitor, and control the Internet" (Henry, Pettyjohn, & York, 2014, p. iii). The program provided funding for secure communication channels and digital security trainings. In 2012–2013, for instance, five projects in the program were targeting Iran, a number only rivaled by those targeting Egypt (Henry et al., 2014, p. 39).

During the same period and throughout the following years, Iranian authorities stepped up their efforts to monitor and control Internet use and communication. Although the repressive atmosphere was unquestionably a result of the challenge that the Green movement had presented to the regime, policies also targeted potential links between foreign actors and Internet and media activists in Iran. In January 2010, the Ministry of the Interior banned contact to more than 60 international media, think tanks, and other organizations considered part of the "soft invasion and overthrow strategies against the Islamic Republic of Iran" (Tait, 2010, para. 9). Contacts between activists in Iran and abroad were strictly monitored and repeatedly provided a pretext for arrests (BBC, 2013). In December 2013, intelligence agencies detained staff members of a popular website on digital technologies that had received international recognition and awards. They were accused of having received foreign funding and of having worked within a "complex security-media network" in relation with foreigners (Center for Human Rights in Iran, 2014). Diaspora activists and organizations working for information freedom were monitored and targeted by malware attacks (Michaelsen, 2016). Workshops on Internet freedom and digital security trainings involving Iranian activists were required to follow security protocols to prevent repercussions for participants upon their return to Iran or for their families in the country.[2]

In addition, Iranian authorities had to respond to technical challenges of the censorship regime resulting from Internet freedom initiatives. Iranian users relied on various circumvention and anonymization tools to bypass Internet filtering. Among the more reliable tools, the Tor browser and Psiphon software enjoyed a growing user base in Iran.[3] Both tools had received funding from the U.S. government and other Western donors. From 2011 onward, Iran started using so-called deep-packet inspection to identify and

[2] Personal observation at several such events during 2014–2016.

[3] In 2011, Iran was the second country worldwide in terms of Tor users. Psiphon reported in 2013 to have up to 1.5 million users per week connecting to its network from Iran. Later, Psiphon did not publish user statistics on Iran for fear of repercussions.

block or throttle encrypted Internet traffic in international connections. In the run-up to the parliamentary and presidential elections in 2012 and 2013, access to services outside Iran that relied on the Secure Sockets Layer was blocked or severely slowed down, restricting the use of prominent applications such as Gmail but also of tools such as Psiphon and Tor (arma, 2011, 2012; Kathuria, 2013). In April 2013, an Iranian computer expert at the University of Isfahan even warned against the use of Psiphon because it would steal information from devices (ASL 19, 2013).

The Iranian state clearly perceived initiatives for Internet freedom as a threat and responded accordingly. The programs provided a justification for intensifying surveillance and pressure against activists, in- and outside Iran. They also prompted the development of technical responses to circumventions of the filtering and monitoring regime. In this sense, the instrumentalization of Internet technology for the purposes of Western democracy promotion not only confirmed the worldview and ideology of the Iranian regime but also pushed it to extend the scope and scale of practices curtailing privacy and freedom of expression in the digital sphere.

Confrontation: Cyberattacks

Iranian threat actors have engaged in cyberattacks against a broad range of domestic and foreign targets, relying on different tools and tactics. A small number of groups with shifting strategies and sophistication active in this field have evolved from amateur to more state-aligned hackers. The direct involvement of the Iranian state in cyberattacks has been documented in only a few cases, but the selection of targets generally corresponds to the ideological and strategic parameters of the Iranian regime. Digital threats against Iranian targets often emanate from the same actors who also aim at foreign adversaries. More important, external cyberattacks against critical state infrastructure have given Iran a clear incentive to develop its own offensive capabilities (Anderson & Sadjadpour, 2018; Villeneuve, Moran, Haq, & Scott, 2013).

On the domestic level, attacks seek to compromise and disrupt the communication of civil society and political opposition. At the height of the 2009 election protests, for instance, websites of Green movement supporters were brought down by so-called distributed-denial-of-service attacks or defacements (OpenNet Initiative, 2013). These rather brute tactics of disrupting online information distribution later shifted to malware campaigns and intrusion attempts against social media networks and e-mail accounts of Iranian activists and journalists, both inside the country and in the diaspora, aiming to monitor and threaten the activities of transnational civil society networks (Michaelsen, 2016). Internationally, operations attributed to Iran range from vandalism to espionage against a large variety of targets in the United States, Europe, and the Middle East (ClearSky Cyber Security, 2015; Villeneuve et al., 2013). At times, attacks against foreign and domestic targets were even interwoven: In 2011, for instance, an Iranian hacker penetrated the Dutch company DigiNotar to issue fraudulent Internet security certificates allowing authorities to spy on the e-mail conversations of millions of Iranian users (Prins, 2011; Sengupta, 2011).

Iran itself has been targeted by cyberattacks and espionage from countries such as France, Russia, Canada, the United Kingdom, and Saudi Arabia. More prominent are undoubtedly the attacks against Iran's nuclear facilities in 2010, which were later attributed to, though not officially acknowledged by, the United

States and Israel. In an attempt to slow down the Iranian nuclear program, both countries infiltrated malicious software into the computers of the Natanz enrichment facility, causing damage to over a thousand centrifuges. The complex campaign, which both countries had prepared secretly for years, was revealed only after an element of the cyberattacks—a computer virus named Stuxnet—accidently escaped and replicated on the Internet (Sanger, 2012, Zetter, 2014). In addition, other equally sophisticated malicious programs targeted information systems in the Iranian oil industry and government institutions, stealing or destroying sensitive data (Erdbrink, 2012; Zetter, 2012b).

The attacks, in the words of former CIA chief Michael Hayden, "crossed the Rubicon" and are considered the first acts of government cyberwarfare against the critical infrastructure of another country (Sanger, 2012; Segal, 2016, p. 111). For the Iranian regime, they signaled that it had to become more assertive in cyberspace and acquire expertise in offensive and defensive tactics. According to a National Security Agency report disclosed with the Snowden files, the attacks may have even given the Iranian authorities an opportunity to learn from the deployed techniques (Greenwald, 2015). In fact, a 2012 attack against the computers of the Saudi Arabian oil company Aramco, attributed to Iranian actors, seems to have been inspired, both technically and in terms of execution, by the Wiper malware that had infiltrated the national Iranian oil company. Security analysts identified elements of Wiper in the software code of the Aramco attack (Perlroth, 2012).

Iran certainly did not need external cyberattacks such as Stuxnet to motivate digital illiberal and authoritarian practices against its own citizens. But the confrontation from outside provided both technical and political opportunities to advance and justify its own capabilities for malware intrusions and other forms of offensive operations. Considering the context of the authoritarian regime and the overlap between actors threatening foreign and domestic targets, the acquired knowledge would also be employed or even tested against targets in the Iranian civil society and political opposition (Anderson & Sadjadpour, 2018, p. 56).

Sanctions: Constraining Access to Technology

Ever since the Islamic Revolution, Iran has been targeted by U.S. sanctions. From the mid-1990s, these sanctions became more comprehensive and reached a peak during the international conflict over Iran's nuclear program, effectively curtailing the country's access to international services, goods, trade, and technologies. After the protests of summer 2009, the U.S. government, realizing the importance of digital technologies, started amending the sanctions regime to facilitate Iranian citizens' access to tools of personal information and communication while preventing the government from obtaining so-called dual-use technology for Internet filtering and surveillance.[4] Targeted sanctions on equipment for Internet controls accompanied exemptions seeking to encourage private companies to provide Iranians with essential services such as antivirus software and secure messaging (Kehl, Maurer, & Phene, 2013; Mehta, 2016).

[4] The 2010 Comprehensive Iran Sanctions, Accountability, and Divestment Act and the 2012 Iran Threat Reduction and Syria Human Rights Act both aimed to curtail the Iranian government's access to technologies that could be used to restrict access to information and freedom of expression (Mehta, 2016, p. 774).

For Iran, the sanctions obstructed the purchase of Western technology for Internet control and surveillance, but they did not make it impossible. In the initial phases of Iranian Internet censorship, Iran used U.S. software such as Websense and SmartFilter, which it obtained apparently on the black market. Later, the use of filtering devices produced by another U.S. company, Blue Coat Systems, was detected in Iran (Marquis-Boire, Anderson, Dale, McKune, & Scott-Railton, 2013). The repression against the protest movement of 2009 also revealed the authorities' use of monitoring technology produced by Nokia Siemens. Following intense pressure by human rights groups and threats of U.S. sanctions, Nokia announced that it would restrict its business with Iran and halt all support for technology it had sold so far (Center for Human Rights in Iran, 2010). In Iran, the sequential purchase and installation of different tools with different capacities led to inconsistencies in the filtering system. Because Iran could not obtain updates to the packages of Western technology it had purchased, tools were used alongside one another, covering different amounts of Internet traffic and bandwidth.[5] In response to tightened sanctions and in the attempt to upgrade its capacities for Internet controls, Iran turned to China for purchasing surveillance technology and policy advice (Stecklow, 2012). Iran was thus able to work around the leverage of U.S. sanctions by cooperating with an "authoritarian sponsor" (Tansey, 2016) who not only had a similar approach to Internet controls but was also able to provide powerful technical solutions, dodging the risk of retaliations from U.S. authorities (Zetter, 2012a).

Although targeted sanctions could not prevent the Iranian state from establishing a sophisticated system of Internet control, the exemptions aiming to facilitate Iranian citizens' access to essential software had a limited effect. The complex and evolving regulations deterred private companies from providing their services to Iran "due to the legal, financial and reputational risks involved" (Mehta, 2016, p. 778). Major companies such as Apple and Google restricted provision of their products for customers in Iran, often in overcompliance with the sanctions regulations (ASL 19, 2017). As a consequence, Iranian users could not access essential updates and security features that would have allowed them to circumvent Internet filtering and surveillance (Frenkel, 2018). This contributed to the impression among users that they were "censored from two sides."[6] In this sense, the U.S. sanctions targeting digital technologies contributed at least indirectly to the authoritarian practices of the Iranian state by preventing users from equipping themselves against privacy invasions and disruptions of information flows. More important, however, for the Iranian government, the sanctions constituted a serious challenge to the country's autonomy and security. Together with the cyberattacks, the sanctions were thus a key driver of the establishment of a national information network that was more resistant to external interference but also more open to state control.

The Politics of Infrastructure: Iran's National Internet

This article has outlined the ways in which the Iranian state's responses to external threats such as Internet freedom promotion, cyberattacks, and sanctions enabled it to advance and justify practices of Internet control. The following description of the national Internet project notes how the regime's threat perceptions coupled with its fundamental values in foreign policy—namely rejection of foreign intrusion and

[5] Personal interview with an Iranian ICT expert and Internet activist, June 2015.

[6] Personal observations during a research visit to Tehran in April 2015.

persistence on independence and sovereignty—translated to the development of infrastructure and an "indigenous" configuration of Internet architecture.

Iranian officials have floated the plan of building a "national" or "clean Internet" for more than a decade. The principal idea was to build a network with limited connections to the global Internet, prioritizing domestic content and services, to protect Iranian communications against external interferences such as attacks, espionage, sanctions, and harmful cultural values. The plan was initially brought up during the first term of President Mahmoud Ahmadinejad (2005–2009), but only limited steps for its implementation were undertaken. In 2010, the Iranian Ministry for Information and Communication Technology ordered public organizations to move content to Iran after U.S. companies ended hosting services for .ir domains. At the time, several government websites were still hosted abroad, in the United States, Canada, and other countries (Article 19, 2016, pp. 11, 26). From 2011, the national Internet was included in Iran's five-year plans guiding the country's development. In addition to relocating content and separating domestic from international Internet traffic, policy plans listed reduced dependency on foreign services, the development of e-government, support of domestic digital business as well as the promotion of Islamic values among the aims of the project.[7]

The Iranian government took important steps to lay out the necessary technical infrastructure for the National Information Network, as the project is officially called. The number of Internet exchange points in the country has been increased, improving the performance and stability of connections. In the region, Iran already has one of the highest rates of domestic connectivity and hosts a comparatively high percentage of the most popular content for Iranian users within its borders (Cowie, 2015).[8] Most of the bandwidth that has been increased in recent years is used for domestic connections (Center for Human Rights in Iran, 2018, p. 27). In addition, Iran has bought and stockpiled IPv4 address space, a limited resource for Internet expansion (Madory, 2015).

After establishing the technical capacity, the government started setting incentives for users to stay on the domestic network through pricing and connection speed. In 2017, 500 high-traffic internal websites were accessible for half the price of access to international content (Center for Human Rights in Iran 2018, 29). These measures actually violated the idea of net neutrality, which stipulates that all Internet traffic should be treated equally. Responding to criticism about this transgression of one of the Internet's foundational principles, Iran's ICT minister Azari Jahromi tweeted a link to the Sponsored Data Program of the U.S. company AT&T, which allows customers to pay for faster data transfer. In fact, the Federal Communications Commission had just dismantled regulations for broadband providers in the United States, enabling them to charge for higher-quality service (Center for Human Rights in Iran, 2017a, 2017b). Whereas net neutrality has been challenged in the United States for economic interests, Iran provides an example of a politically motivated subversion of the net neutrality principle. Yet the Iranian government was able to use steps taken in the United States as a justification for its own policies.

[7] See, for instance, the fifth development plan of the Islamic Republic of Iran at https://www.mcls.gov.ir/icm_content/media/law/634654234865929690.pdf.

[8] In 2015, Iran hosted 65% of the most popular Web content in the country. For comparison, Qatar hosted 9% and Saudi Arabia 15%. Worldwide, China hosted 85%, Russia 55%, and the United States 90%.

Popular foreign services such as Google and Telegram have so far resisted Iranian requests to shift servers into the country, and the government sponsors the development of domestic equivalents for search engines, social networks, e-mail providers, and video-sharing platforms. These applications aim to channel users to the domestic network and decrease international traffic (Center for Human Rights in Iran, 2018, p. 44). State-supported services enjoy limited success, because Iranian users do not trust their security and prefer international platforms (Esfandiari, 2018).

Advocacy-oriented research on Iran's national Internet highlights the implications for human rights and freedom of expression. Businesses in Iran are subject to the country's legislation, with flexibly framed definitions of cybercrimes. Data hosted on Iranian servers are exposed to the scrutiny of state authorities (Article 19, 2016; Center for Human Rights in Iran, 2018).

The possibility to monitor and control digital communications more easily is certainly a central motivation for "domesticating" the Internet. Security agencies seem to be closely involved in the project (Center for Human Rights in Iran, 2018). Taking into account external challenges such as cyberattacks and targeted sanctions that threaten information security and digital development in Iran, the changes in the country's Internet infrastructure in fact reveal a dual intent: building a network that facilitates state oversight and control but also economic growth, security for commerce, and efficient administration despite international sanctions and the risk of service interruptions. As such, the project needs to be seen in the context of Supreme Leader Khamenei's call for a "resistance economy" emphasizing self-sufficiency and domestic production in defense against international sanctions and the isolation of the country (Smyth, 2016). Iran's national Internet project thus underlines how international politics led to the establishment of a technical infrastructure that lends itself to the expansion of digital authoritarian and illiberal practices.

Conclusion

This article investigates how the inclination and capability of the Iranian state to engage in measures of Internet control were shaped by its position and struggles in the international system, particularly its enduring conflict with the United States. The regime transformed (perceived) foreign threats to its stability and strategic interests into stronger state control over the Internet. Western democracy promotion, cyberattacks, and sanctions enabled the Iranian state to further develop and justify digital illiberal and authoritarian practices such as surveillance and censorship. International politics showed effects on three levels: the decisions of the state to improve capacities of Internet control, the actual degree of capacities, and their strategic use and application. The responses of the Iranian state thus reveal important dynamics of adaptation and learning.

First, the U.S.-dominated Internet freedom agenda confirmed the regime's view of media as instruments of foreign interference. The professed support of Western governments for Internet activists and circumvention tools motivated state authorities to increase surveillance and persecution of critical online activity and to improve technical capacities for Internet monitoring and filtering. Second, the cyberattacks against crucial state infrastructure spurred the development of Iran's offensive capabilities for malware attacks and infiltrations, and they even provided Iran with an opportunity to learn from its adversaries.

These capacities could then be used to threaten foreign opponents and domestic dissidents alike. Third, the U.S. sanctions, constraining access to global trade, services, and technology, were seen as a serious threat to Iran's autonomy and sovereignty. In a form of authoritarian collaboration, Iran turned to China as a supplier of performant censorship technology. It also intensified the development of domestic software and applications. Most important, finally, the sanctions and cyberattacks pushed the state further in its project to build a national information network that is both more resistant to external interferences and susceptible to state control. The national Internet clearly represents an attempt to reestablish state sovereignty through a particular configuration of Internet architecture.

The case of Iran exemplifies the notion that the decisions and strategies of authoritarian states seeking to control and use the Internet to their benefit cannot be separated from their position and struggles in the international environment. As a global communication structure, the Internet carries political interests and ideas that are built into the technology, potentially provoking resistance and conflict. For scholars studying authoritarian resilience, a focus on the international politics of the Internet helps to explain important mechanisms in the exercise and maintenance of state power, complementing existing approaches on learning and diffusion or authoritarian sponsorship. For research on authoritarian Internet policies, a widening of the analytical scope to the international dimension allows us to discern how practices of control, surveillance, and censorship are stimulated, produced, and transferred in a global context, involving both democratic and authoritarian states as well as civil society and the private sector. As issues of global Internet governance and infrastructure regulation increasingly become a field for broader geopolitical and socioeconomic contention, the role of digital technologies in international politics clearly merits further attention.

References

Ambrosio, T. (2010). Constructing a framework of authoritarian diffusion: Concepts, dynamics, and future research. *International Studies Perspectives*, *11*(4), 375–392. doi:10.1111/j.1528-3585.2010.00411.x

Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat: Espionage, sabotage, and revenge.* Washington, DC: Carnegie Endowment for International Peace. Retrieved from http://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

arma. (2011, September 14). Iran blocks Tor; Tor releases same-day fix [Web log post]. *Tor.* Retrieved from https://blog.torproject.org/iran-blocks-tor-tor-releases-same-day-fix

arma. (2012, February 16). Obfsproxy: The next step in the censorship arms race [Web log post]. *Tor.* Retrieved from https://blog.torproject.org/obfsproxy-next-step-censorship-arms-race

Article 19. (2013). *Computer crimes in Iran: Online repression in practice.* London, UK: Author. Retrieved from https://www.article19.org/data/files/medialibrary/37385/Computer-Crimes-in-Iran-.pdf

Article 19. (2016). *Tightening the net: Internet security and censorship in Iran. Part 1: The National Internet Project.* London, UK: Author. Retrieved from https://www.article19.org/data/files/medialibrary/38316/The-National-Internet-AR-KA-final.pdf

ASL 19. (2013). Information controls: Iran's presidential elections. Retrieved from https://asl19.org/cctr/iran-2013election-report/

ASL 19. (2017, January 17). List of services that are not available to Iranian Internet users. Retrieved from https://asl19.org/en/blog/2017-01-17-list-of-services-tech-sanctions.html

Azimi, N. (2007, July 24). Hard realities of soft power. *New York Times Magazine.* Retrieved from http://www.nytimes.com/2007/06/24/magazine/24ngo-t.html?pagewanted=all

Bank, A., & Edel, M. (2015, June). *Authoritarian regime learning: Comparative insights from the Arab uprisings* (GIGA Working Papers No. 274). Hamburg, Germany: German Institute of Global and Area Studies. Retrieved from https://www.giga-hamburg.de/de/system/files/publications/wp274_bank-edel.pdf

BBC. (2013, January 28). Iran arrests 11 journalists with foreign contacts. Retrieved from http://www.bbc.com/news/world-middle-east-21230687

BBC Persian. (2009, March 19). Revolutionary guards: Online networks for overthrow have been destroyed. Retrieved from http://www.bbc.com/persian/iran/2009/03/090319_he_pasdars_internet.shtml

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford, UK: Oxford University Press.

Carr, M. (2016). *U.S. power and the Internet in international relations: The irony of the information age*. New York, NY: Palgrave Macmillan.

Center for Human Rights in Iran. (2010, October 6). Shirin Ebadi: Nokia Siemens' action a major accomplishment for Iranians and for the people of the world. Retrieved from https://www.iranhumanrights.org/2010/10/shirin-ebadi-nokia-siemens-action-a-major-accomplishment-for-iranians-and-for-people-of-the-world/

Center for Human Rights in Iran. (2014, June 20). Eleven Internet professionals sentenced to one to eleven years in prison. Retrieved from https://www.iranhumanrights.org/2014/06/cyber-activists/

Center for Human Rights in Iran. (2017a, December 7). Rouhani Admin's new "fair usage" Internet price rates violate net neutrality. Retrieved from https://www.iranhumanrights.org/2017/12/rouhani-admins-new-fair-usage-internet-price-rates-violate-net-neutrality/

Center for Human Rights in Iran. (2017b, December 21). US repeal of net neutrality harms Internet freedom at home and abroad. Retrieved from https://www.iranhumanrights.org/2017/12/us-repeal-of-net-neutrality-harms-internet-freedom-at-home-and-abroad/

Center for Human Rights in Iran. (2018, January). *Guards at the gate: The expanding state control over the Internet in Iran.* New York, NY: Author. Retrieved from https://www.iranhumanrights.org/wp-content/uploads/EN-Guards-at-the-gate-High-quality.pdf?x96855

Christensen, C. (2011). Discourses of technology and liberation: State aid to net activists in an era of "Twitter revolutions." *Communication Review*, *14*(3), 233–253. doi:10.1080/10714421.2011.597263

ClearSky Cyber Security. (2015, June). *Thamar Reservoir: An Iranian cyber-attack campaign against targets in the Middle East.* Tel Aviv, Israel: Author. Retrieved from http://www.clearskysec.com/wp-content/uploads/2015/06/Thamar-Reservoir-public1.pdf

Clinton, H. R. (2010, January 21). Remarks on Internet freedom. Retrieved from https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Cowie, J. (2015, April). *Middle Eastern content hosting in 2015.* Presentation at MENOG 15, Dubai, United Arab Emirates. Retrieved from http://www.menog.org/presentations/menog-15/309-Cowie_MENOG_15.pdf

Deibert, R., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance: A Review of Multilateralism and International Organizations*, *18*(3), 339–361.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). *Access contested: Security, identity and resistance in Asian cyberspace*. Cambridge, MA: MIT Press.

DeNardis, L. (2014). *The global war for Internet governance.* New Haven, CT: Yale University Press.

Diamond, L. (2010). Liberation technology. *Journal of Democracy*, *21*(3), 69–83.

Ebert, H., & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, *34*(6), 1054–1074. doi:10.1080/01436597.2013.802502

Ehteshami, A., Hinnebusch, R., Huuhtanen, H., Raunio, P., Warnaar, M., & Zintl, T. (2013). Authoritarian resilience and international linkages in Iran and Syria. In S. Heydemann & R. Leenders (Eds.), *Middle East authoritarianisms: Governance, contestation, and regime resilience in Syria and Iran* (pp. 222–244). Redwood City, CA: Stanford University Press.

Erdbrink, T. (2012, May 29). Iran confirms attack by virus that collects information. *The New York Times*. Retrieved from http://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=1&hp

Esfandiari, G. (2018, January 20). After protests, Iran leadership pushes hard for "homegrown" apps. *Radio Free Europe/Radio Liberty*. Retrieved from https://www.rferl.org/a/iran-social-media-homegrown-apps-instagram-telegram/28986523.html

Finkel, E., & Brudny, Y. M. (2012). No more colour! Authoritarian regimes and colour revolutions in Eurasia. *Democratization*, *19*(1), 1–14. doi:10.1080/13510347.2012.641298

Frenkel, S. (2018, January 2). Iran blocks access to social media tools. *The New York Times*. Retrieved from https://www.nytimes.com/2018/01/02/technology/iran-protests-social-media.html

Gharbia, S. B. (2010, September 17). The Internet freedom fallacy and the Arab digital activism [Web log post]. *Nawaat.* Retrieved from https://nawaat.org/portail/2010/09/17/the-internet-freedom-fallacy-and-the-arab-digital-activism

Glasius, M. (2018). What authoritarianism is . . . and is not: A practice perspective. *International Affairs*, *94*(3), 515–533. doi:10.1093/ia/iiy060

Goebel, C. (2013). The information dilemma: How ICT strengthen or weaken authoritarian rule. *Statsvetenskaplig Tidskrift*, *115*(2013), 367–384. Retrieved from https://ssrn.com/abstract=2108787

Greenwald, G. (2015, February 10). NSA claims Iran learned from Western cyberattacks. *The Intercept*. Retrieved from https://theintercept.com/2015/02/10/nsa-iran-developing-sophisticated-cyber-attacks-learning-attacks

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, *13*(1), 42–54. doi:10.1017/S1537592714003120

Hall, S. G., & Ambrosio, T. (2017). Authoritarian learning: A conceptual overview. *East European Politics*, *33*(2), 143–161. doi:10.1080/21599165.2017.1307826

Henry, R., Pettyjohn, S., & York, E. (2014). *Portfolio assessment of the Department of State Internet Freedom Program.* Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR794.html

Hoffmann, B. (2015). The international dimension of authoritarian regime legitimation: Insights from the Cuban case. *Journal of International Relations and Development*, *18*(4), 556–574. doi:10.1057/jird.2014.9

Hussain, M. M. (2013). Digital infrastructure politics and Internet freedom stakeholders after the Arab Spring. *Journal of International Affairs*, *68*(1), 37–56.

Hussain, M. M., & Howard, P. N. (2014). *State power 2.0: Authoritarian entrenchment and political engagement worldwide*. Surrey, UK: Ashgate.

Iran Human Rights Documentation Center. (2010). *Violent aftermath: The 2009 election and repression of dissent in Iran.* Retrieved from http://www.iranhrdc.org/english/publications/reports/3161-violent-aftermath-the-2009-election-and-suppression-of-dissent-in-iran.html

Josua, M., & Edel, M. (2015). To repress or not to repress—Regime survival strategies in the Arab Spring. *Terrorism and Political Violence*, *27*(2), 289–309. doi:10.1080/09546553.2013.806911

Kathuria, K. (2013, October 28). Psiphon and the 2013 Iranian election [Web log post]. *Psiphon.* Retrieved from https://www.psiphon3.com/en/blog/psiphon-iranian-election-2013.html

Kehl, D., Maurer, T., & Phene, S. (2013). Translating norms to the digital age. Technology and the free flow of information under U.S. sanctions. Washington, DC: New America Foundation. Retrieved from https://www.newamerica.org/oti/policy-papers/translating-norms-to-the-digital-age

Khamenei, A. (2016, June 3). Speech on the 27th anniversary of the death of Imam Khomeini. Retrieved from http://farsi.khamenei.ir/speech-content?id=33259

Khamenei, A. (2017, February 15). Statement in meeting with people from Azerbaijan. Retrieved from http://farsi.khamenei.ir/speech-content?id=35690

Kian, A. (1995). L’invasion culturelle occidentale: Mythe ou réalité? [The Western cultural invasion: Myth or reality?]. *Cemoti*, *20*. Retrieved from http://journals.openedition.org/cemoti/1668

Koesel, K. J., & Bunce, V. J. (2013). Diffusion-proofing: Russian and Chinese responses to waves of popular mobilizations against authoritarian rulers. *Perspectives on Politics*, *11*(3), 753–768. doi:10.1017/S1537592713002107

Levitsky, S., & Way, L. A. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War*. New York, NY: Cambridge University Press.

MacKinnon, R. (2011). China’s “networked authoritarianism.” *Journal of Democracy*, *22*(2), 32–46. doi:10.1353/jod.2011.0033

Madory, D. (2015, April 6). *IPv4 address market takes off.* Manchester, NH: Oracle Dyn. Retrieved from https://dyn.com/blog/ipv4-address-market-takes-off/

Marquis-Boire, M., Anderson, C., Dalek, J., McKune, S., & Scott-Railton, J. (2013, July 9). *Some devices wander by mistake. Planet Blue Coat redux.* Toronto, Canada: Citizen Lab and Canada Centre for

Global Security Studies. Retrieved from https://citizenlab.ca/storage/bluecoat/CitLab-PlanetBlueCoatRedux-FINAL.pdf

McCarthy, D. R. (2015). *Power, information technology, and international relations technology: The power and politics of U.S. foreign policy and the Internet.* New York, NY: Palgrave Macmillan.

McCarthy, D. R. (2017). *Technology and world politics: An introduction.* London, UK: Routledge.

Mehr News. (2017, October 24). 47 million Iranians use mobile Internet. Retrieved from https://www.mehrnews.com/news/4140564/

Mehta, P. P. (2016). Sanctioning freedoms: U.S. sanctions against Iran affecting information and communications technology companies. *University of Pennsylvania Journal of International Law*, *37*(2), 763–812.

Michaelsen, M. (2015). Beyond the "Twitter-revolution": Internet and political change in Iran. In P. Weibel (Ed.), *Global activism: Art and conflict in the 21st century* (pp. 384–395). Cambridge, MA: MIT Press.

Michaelsen, M. (2016). Exit and voice in a digital age: Iran's exiled activists and the authoritarian state. *Globalizations*, 15(2), 248–264. doi:10.1080/14747731.2016.1263078

Morozov, E. (2011). *The net delusion: How not to liberate the world*. London, UK: Allen Lane.

OpenNet Initiative. (2013, February 15). *After the Green movement: Internet controls in Iran 2009–2012.* Retrieved from www.opennet.net/iranreport2013

Peksen, D., & Drury, A. C. (2010). Coercive or corrosive: The negative impact of economic sanctions on democracy. *International Interactions*, *36*(3), 240–264. doi:10.1007/s12142-009-0126-2

Perlroth, N. (2012, August 24). Among digital crumbs from Saudi Aramco attack images of burning U.S. flag. *The New York Times*. Retrieved from https://bits.blogs.nytimes.com/2012/08/24/among-digital-crumbs-from-saudi-aramco-cyberattack-image-of-burning-u-s-flag

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, *14*(3), 399–441. doi:10.1177/030631284014003004

Pitney, N. (2012, March 20). Obama Nowruz video directed at Iran people decries "electronic curtain" on Persian New Year. *Huffington Post*. Retrieved from https://www.huffingtonpost.com/2012/03/20/obama-nowruz-message-video-iran-electronic-curtain_n_1367441.html

Pleming, S. (2009, June 16). U.S. State Department speaks to Twitter over Iran. *Reuters.* Retrieved from https://www.reuters.com/article/us-iran-election-twitter-usa/u-s-state-department-speaks-to-twitter-over-iran-idUSWBT01137420090616

Price, M. (2012). Iran and the soft war. *International Journal of Communication*, *6*(2012), 2397–2415.

Prins, J. R. (2011, September 5). *DigiNotar certificate authority breach "Operation Black Tulip"* (Interim Report). Delft, Netherlands: Fox-IT. Retrieved from http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1/rapport-fox-it-operation-black-tulip-v1-0.pdf

Rahimi, B. (2011). The antagonistic social media: Cyberspace in the formation of dissent and consolidation of state power in postelection Iran. *Communication Review*, *14*(3), 158–178. doi:10.1080/10714421.2011.597240

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research*, *52*(3), 338–351. doi:10.1177/0022343314555782

Sanger, D. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. Retrieved from http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

Segal, A. (2016). *The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age*. London, UK: Hachette.

Sengupta, S. (2011, September 11). Hacker rattles security circles. *The New York Times*. Retrieved from http://www.nytimes.com/2011/09/12/technology/hacker-rattles-internet-security-circles.html?pagewanted=all&_r=0

Smyth, G. (2016, April 19). Deciphering the Iranian leader's call for a "resistance economy." *The Guardian*. Retrieved from https://www.theguardian.com/world/iran-blog/2016/apr/19/iran-resistance-economy-tehranbureau

Sreberny, A. (2013). Too soft on "soft war": Commentary on Monroe Price's "Iran and the Soft War." *International Journal of Communication*, *7*(2013), 801–804.

Stecklow, S. (2012, March 22). Chinese firm helps Iran spy on citizens. *Reuters*. Retrieved from http://www.reuters.com/article/us-iran-telecoms-idUSBRE82L0B820120322

Tait, R. (2010, January 5). Iran bans contact with foreign organizations, including the BBC. *The Guardian.* Retrieved from https://www.theguardian.com/world/2010/jan/05/iran-bans-contacts-foreign-organisations

Tansey, O. (2016). *International dimensions of authoritarian rule.* Oxford, UK: Oxford University Press.

Tezcür, G. M. (2012). Democracy promotion, authoritarian resiliency, and political unrest in Iran. *Democratization*, *19*(1), 120–140. doi:10.1080/13510347.2012.641296

Villeneuve, N., Moran, N., Haq, T., & Scott, M. (2013) *Operation Saffron Rose*. Milpitas, CA: FireEye. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

Warnaar, M. (2013). *Iranian foreign policy during Ahmadinejad*. New York, NY: Palgrave Macmillan.

Wood, R. M. (2008). "A hand upon the throat of the nation": Economic sanctions and state repression, 1976–2001. *International Studies Quarterly*, *52*(3), 489–513. doi:10.1111/j.1468-2478.2008.00512.x

Zetter, K. (2012a, July 12). FBI investigating major Chinese firm for selling spy-gear to Iran. *Wired*. Retrieved from https://www.wired.com/2012/07/fbi-zte/

Zetter, K. (2012b, August 29). Wiper malware that hit Iran left possible clues of its origins. *Wired*. Retrieved from https://www.wired.com/2012/08/wiper-possible-origins

Zetter, K. (2014). *Countdown to zero day: Stuxnet and the launch of the world's first digital weapon*. New York, NY: Broadway Books.