Two Can Play At That Game: Social Media Opportunities in Azerbaijan for Government and Opposition

Katy Pearce
University of Washington, Seattle

Abstract: Much has been written on the ways in which the Internet benefits opposition movements, in particular in authoritarian regimes. And while some acknowledge that the Internet also provides opportunities for authoritarian governments as well, few have looked at the Internet and social media as a space for back-and-forth actions between the sides. In Azerbaijan, social media allows both the ruling regime and oppositionists to engage with each other and Azerbaijani citizens in new ways. Social media provides the regime with an alternative medium to harass the opposition and demonstrate its power to the citizenry. And while there is a social media presence, the traditional opposition parties do not leverage all affordances of it, however oppositionists not affiliated with traditional parties are leveraging social media to build audiences and engage in action. While the regime is currently “winning” the social media battle through the use of its resources, the new and creative ways that oppositionists are using social media for connective action could prove to be a successful means of dissent.

Katy Pearce is Assistant Professor in the Department of Communication at University of Washington, Seattle, Box 353740 Seattle, WA 98195, email: kepearce@uw.edu.
The authoritarian state of Azerbaijan has a unique way of regulating the Internet and social media to maximize its opportunities for simultaneously promoting itself while deterring dissent. Instead of using high-level filtering, it instead uses psychological techniques to create an environment of self-censorship (and increasingly is using policy mechanisms to enforce the psychological controls.) The government also monitors and punishes social media-enabled dissent. Nonetheless, oppositionally-minded Azerbaijanis use social media as a promotional tool, an information dissemination medium, and for some – though not the traditional opposition parties – an organizational tool.

This article will describe how the opposition uses social media for organizing, using the Connective Action framework to understand different opposition uses of social media for action, and explain how the government controls the online space. Analysis of how the two sides use the Internet enhances understanding of how social media can enrich not only our understanding of the Azerbaijani political scene, but also how social media and politics intersect in more authoritarian contexts, a perspective that is sorely missing from current writing on social media and politics. Social media has enabled both the government and the opposition to engage with each other and Azerbaijani citizens. For the government, social media provides an alternative medium to toy with the opposition and demonstrate its power to the citizenry. The traditional opposition, on the other hand, does not effectively use social media to engage it audience. However, oppositionists not affiliated with traditional parties are leveraging social media to build audiences and engage in action.

Background

personalist-clientelist nature of Aliyev’s rule, where patronage-based elite factions demonstrate loyalty and become dependent on resources allocated by the ruling party; 2) deficient stateness and endemic corruption, which dominate all aspect of political life; and 3) a marginalized political opposition, which exists but represents few organized interests. Additionally, the citizens of Azerbaijan experience a general sense of apathy and fear and a lack of trust in others. As such, Azerbaijani society is self-censoring.

The Internet in Azerbaijan

In Azerbaijan, the government has nearly total control of the mainstream media. Accordingly, in the last few years, many oppositionally-minded Azerbaijanis have turned to the Internet to express their political views. With the growth of social media, especially Facebook (between 13-18 percent of Azerbaijanis had a Facebook account as of late 2013), this sort of political deliberation has increased. As the openness of the Internet became an attractive space for activists, the Azerbaijani government seemingly took notice and began formulating a policy to control it. Like in the print media sphere, the Azerbaijani government understood that allowing some independence can provide benefits. One argument along these lines is that authoritarian states make policies and have bureaucrats to implement them. Independent media is one of the only ways that authoritarian leaders can verify that the bureaucrats are doing their jobs. With the Internet and social media, a little bit of freedom can provide the government with insight into what the opposition elite are thinking, as well as an excellent and systematic monitoring tool. Some freedom on the


Internet can also allow the Azerbaijani government to appear democratic.\textsuperscript{10} However, the Azerbaijani government does have to control the Internet and social media in order to ensure that dissent does not go beyond what it considers a safe level. In the second half of this paper, I will apply Deibert and Rohozinski’s\textsuperscript{11} framework from their study of the Russian-language Internet to Azerbaijan by dividing the techniques used by governments for Internet censorship and control into three “generations.” The Azerbaijani government engages in each of these generations. But first, a description of how the opposition does and does not use the Internet for organizing will be presented.

**Opposition Background**

The opposition in Azerbaijan is both marginalized and divided.\textsuperscript{12} However, despite its fragmentation, the opposition is networked. Connections, often of a personal nature, exist between individuals and groups within the larger movement, despite subdivisions organizationally. These ties create a web that is more difficult to destroy.

Moreover, these information relationships are essential to understand politics in Azerbaijan. To “make sense of political processes and outcomes in such contexts, paying attention to the formal institutions that are typically the focus of political scientists is inadequate; in addition—or instead—one must study informal institutions and interactions.”\textsuperscript{13}

Being networked creates efficiency advantages over more hierarchical forms of organization.\textsuperscript{14} Networks are light on their feet. Information transfers reliably and efficiently through them.\textsuperscript{15} Moreover, networked forms of organization have greater trust amongst individuals,\textsuperscript{16} reciprocity\textsuperscript{17}, and more opportunities for learning from one another.\textsuperscript{18}


\textsuperscript{12} Guliyev. 2012. “Political Elites in Azerbaijan.”


\textsuperscript{17} Powell. 1990. “Neither Market nor Hierarchy.”

networks such as these are essential for mobilization in non-democracies. The web of personal ties between oppositionally-minded people has traditionally been maintained offline. However, new technologies provide opportunities for these ties to be maintained and reaffirmed virtually.

**Impact of the Internet on organizing**

The Internet and social media have had an impact on interpersonal relationships. Information and communication technologies can foster connectedness and socialbility. The Internet has also affected organizational relationships. And specifically, new opportunities and challenges for social movements have emerged. The Internet reduces barriers for creating, organizing, and participating without co-presence and at a reduced cost, and in Azerbaijan, where freedom of assembly is restricted, being able to organize without co-presence is a tremendous asset to organizations. The reduction in cost is also useful for Azerbaijani oppositionists because one of the government’s strongest tools against them is economic.

However, these same affordances provided by the Internet also threaten traditional social movement organizations because the barriers for competitors are also reduced. Established opposition parties no longer hold the monopoly on countering the government. An individual or a loosely organized group can create and organize social activism much more easily than in the pre-Internet era.

Social media and social networking sites are especially important for social movements – regardless if they are an established opposition group, individuals, or loosely organized groups. Broadly defined, a social network site (SNS) is a “networked communication platform in which participants 1) have uniquely identifiable profiles that consist of user-supplied content, content provided by other users, and system-level data; 2) can publicly articulate connections that can be viewed and traversed by others; and 3) can consume, produce, and interact with streams of user-generated content.”

---


Social networking sites are ideal for generating and affirming interpersonal interaction, broadening social ties, and providing information about how to become involved (Valenzuela et al. 2009). They also allow individuals and organizations to better manage their social networks and connect with new individuals. Further, Facebook is like an information hub, and users can receive mobilizing information and encounter greater opportunities to engage by following particular personalities and joining groups. Users can also express their political opinions on social media. In fact, Valenzuela found that social media use for political opinion expression and activism were significant predictors of protest behavior.

**Opposition Social Media Organizational Structure**

These particular affordances of the Internet and social media are important because they can enable a new type of social movement collective action form: connective action, especially in an era when younger people are shifting away from identifying with organizations to engaging civically through “simple, everyday discourses anchored in lifestyles and shared with social networks.” (Similar is the idea of “networked individualism” as described by Rainie and Wellman in which technology enables a new osmotic self that absorbs elements from multiple networks, which is personalized, while still networked.) This individualization means that individuals are less guided by norms and collective identities. Imagine campaigns, for example, such as a young woman holding a hand-written sign that states “I have type I diabetes. How can I afford college when I may not be able to afford my insulin? I am the 99%” being shared by sympathetic others. Or in the case of Azerbaijan, personal opinions and statements about the political situation, rather than party alliances, being popular on Facebook or photographs of the families of political detainees.

---


27 Valenzuela. 2013. “Unpacking the Use of Social Media for Protest Behavior.”


being shared on social media – this is not organizationally-sponsored, but
driven by individuals empathetic to other individuals’ plights. This demand
for personalized relations with causes or organizations makes social
media more central as an organizing tool. “When people who seek more
personalized paths to concerted action are familiar with practices of social
networking in everyday life, and when they have access to technologies
from mobile phones to computers, they are already familiar with a different
logic of organization: the logic of connective action... the recognition of
digital media as organization agents... taking public action or contributing
to a common good becomes an act of personal expression.”

Traditional organizational structures (what Bennett and Segerberg
call organizationally brokered networks\textsuperscript{31}) are noteworthy for strong
organizational coordination of action (especially with regard to resource
allocation and distribution) and formalized relationships with followers
(members). The organizations are greatly concerned with getting indi-
viduals to join when the cost of participating outweighs the benefits.
Rhetoric engages collective action frames rather than personalized ones.
Social media is used to reduce communication and coordination costs, but
it does not fundamentally change the logic of participation or action. This
does not mean that these traditional organizations do not use social media,
rather it is used as a tool rather than an organizational agent. In Azerbaijan,
the traditional opposition parties are examples of this. And while the best
known individuals have many followers, friends, or likes, there is very
little personalized interaction with audience members. It should be noted
that in Azerbaijani parties, as in many post-Soviet political parties, a great
deal of party activity \textit{is} focused on individuals. Because of this, Bennett
and Segerberg’s description of organizational brokered networks, derived
from Western organizations, may not seem appropriate. Nonetheless, those
individuals receiving the focus are essentially symbols of the organization.

However, with the introduction of digital media, the logic of this
sort of organization can change. Through the organizational processes
of social media, the symbolic construction of a united “we” and organ-
ization to support that “we” is unnecessary.\textsuperscript{32} Motivation to join and
participate may be different in digitally-enabled networks and cooperation
is voluntary.\textsuperscript{33} Based in the production and sharing of content – the way
that individuals associate and organize with one another is quite different

\textit{Information, Communication \\& Society} 15 (5) (June): 739–768. doi:10.1080/136911
8X.2012.670661.


\textsuperscript{33} Yochai Benkler. 2006. The Wealth of Networks: How Social Production Transforms Mar-
than in non-digitally-enabled networks. This co-production and co-distribution is personalized expression that allows for symbolic inclusiveness and technological openness. This sort of engagement can occur either in organizationally-enabled networks or in crowd-enabled networks.

The first type of connective action is with organizationally enabled networks, with loose organizational coordination of action around a general set of issues and organizationally generated inclusive personal action frames with some moderation of personal expression. Social media is part of organizing, but there is still an organization in the background. In Azerbaijan, examples include groups like N!DA that have formal structures, but strongly engage with social media for more than organizational purposes as well as the REAL (Republican Alternative) organization, which is mostly an offline organization, but its leadership uses social media beyond information dissemination and recruitment. The social media presence of this sort of organization is much more organizationally-based than individually-based, as network-building mechanisms that allow individuals to contribute, bringing more agency to individuals than as it is with traditional organizations.

Full connective action, which Bennett and Segerberg call crowd-organized/technology-enabled, comes from self-organizing networks, which are individuals with little or no organizational coordination of action and collective action is entirely about personal action frames. Social media is an integrative organizational mechanism and possibly the most visible activity of the network. These individuals are very much engaged in personal expression and have a strong and personal voice in their social media content. Individuals activate their own followers and social networks. These individuals have the largest social media audience and influence of anyone in Azerbaijan.

There is certainly a class of “Internet Celebrities” in Azerbaijan, individuals with large social media followings that have the ability to set the tone and spread information. There are pro-government celebrities, but the opposition has many as well at all three levels: organizationally brokered networks, organizationally enabled networks, and crowd-enabled networks. Again, the focus on individuals within post-Soviet politics should be recalled while considering this sort of activity.

Some of these individuals have notable foreign audience as well and can be considered “networked microcelebrities.” A networked

---

microcelebrity activist “is a politically motivated actor who successfully uses affordances of social media to engage in a presentation of his or her political and personal self to garner attention to a cause.”  

Further, “networked microcelebrity activism refers to politically motivated noninstitutional actors who use affordances of social media to engage in the presentation of their political and personal selves to garner public attention to their cause, usually through a combination of testimony, advocacy, and citizen journalism.” Zeynep Tufekci argues that these people serve a particular role in a movement - often writing in a bridging language (English) - to gain the attention of a global audience, but this may also have a negative consequence within the movement because of the opportunities provided by global microcelebrity. Dahlgren’s idea of “online public intellectuals” is also pertinent to understanding these individuals. According to Dahlgren, these public intellectuals play a significant role, especially within alternative politics, and digital media allows for amplification of their messages. These public intellectual microcelebrities allow for effective activation of social networks for connective action.

Examples of Connective Action

Protest Events

Connective action networks can be particularly effective in protest events. (Although as Henry Hale notes, social media may not have a primary role in unrest. Nonetheless, I argue that in the 2013 cases described here, social media was central to organizing.) Since early 2013, there have been a number of protest actions organized primarily via Facebook without any sponsorship from any of the traditional opposition parties, rather individuals spread through their personal social networks. Moreover, there was a personalized action frame: conscripts’ deaths because of hazing and the government’s attempts to cover up these deaths. Pictures of soldiers were spread on social networks and personalized catch phrases were commonly shared on image memes or as Facebook status. While attendance at these protests was sometimes large and sometimes not, the number of individuals saying that they were going to attend an event via Facebook was quite high, especially for such a public statement. Over time, the protests’ focus

39 Tufekci. 2013. “‘Not This One’.”
41 Bennett and Alexandra Segerberg. 2013. The Logic of Connective Action.
moved away from conscript deaths and into more generalized protest, and perhaps not coincidentally, support decreased.

Fundraising

After individuals received fines for participating in the winter 2013 protest actions, some individuals, not affiliated with traditional opposition parties, created a campaign to raise small amounts of money to pay off the fines. In less than a week, they raised 10,500 AZN (US$13,000). These efforts were notable for connective action for two reasons: first, the fundraising was for individuals rather than for a cause. Secondly, the focus on pocket change (the campaign was called 5 cents), made it accessible for individuals wanting to engage.

After the success of the donate change campaign, the government put greater restrictions on fundraising for NGOs and charities. Individuals, again, not affiliated with traditional opposition parties, started a new fundraising effort through selling personal photographs, the monetary exchange representing a donation. While this is an illustration of personal action frames by these individuals, it should be noted that this sort of microcelebrity behavior fits in well in post-Soviet political culture where individuals are symbolic of organizations as well as within personal action frames in connective action.

Effect of Connective Action Networks

The result of connective action is that seemingly disjointed networks can achieve coherent organizational forms in that they develop capacities for resource allocation and distribution; they response to external short-term events; and they also can create long-term adaptive resources. Because of this, they are, essentially, an organization, despite not being a cohesive unit. As an illustration, protests organized via connective action networks tend to scale up more quickly, have large participation, are quite flexible, and are more inclusive than traditional protests.

These informal connective collaborations through social media are challenging the meaning of civil society. Milan and Hintz even argue that decentralized activists organized online (connective) will “play a crucial role in building the digital backbone of contemporary social movements, experimenting with technological infrastructure, and enabling innovative forms of organization and citizen action typical of the digital age.”

Although, it should be noted that the sustainability of connective action networks remains to be seen.

Additionally, there seems to be a conflict between the traditional organizational networks and the newer connective action networks. Today in Azerbaijan, due in part to the Internet, traditional opposition parties no longer have a monopoly over the opposition. Instead, the connective action individuals and their networks that oppose the government make it possible to disseminate information and build an audience without the infrastructure of a formal organization. However, as Zeynep Tufekci suggests, more ad-hoc connective action networks may be hindered and specifically have difficult sustaining themselves because they are not building network internalities and organizational capacity due to their digitally-enabled coordinating. While it remains to be seen if these networks will be sustainable, there is some evidence that they are already having some impact in Azerbaijani politics.

At this point, the established opposition parties may want to consider some of the successful collective action that non-traditional oppositionally-minded Azerbaijani are engaging in. While it is possible that these successes are partially attributable to the lack of affiliation with formal parties, they do demonstrate that social media can have concrete and sometimes meaningful outcomes. The non-traditional oppositionists may have aspirations for larger political actions and should consider these successes as well to determine best practices and leverage their triumphs to continue engaging the social media users that already have done so. Both traditional and non-traditional opposition should consider the potential power of the “real” and virtual social networks that they have and the opportunity to grow their audiences and followers could be better utilized with strategic thinking about how to best organize and promote activities and events.

**Government Internet and Social Media Policies**

The Azerbaijani government controls the Internet and social media at multiple levels. Using Deibert and Rohozinski’s three “generations” framework, I will describe these levels and provide examples of each.

**First Generation**

First-generation controls “focus on denying access to specific Internet resources by directly blocking access to servers, domains, keywords, and


Filtering and Blocking

In Azerbaijan, filtering with software or hardware is fairly uncommon. However, the technology does exist, as there are some recent occurrences of filtering. However, there are some exceptions, specifically Azerbaijani secondary schools’ Internet access is filtered for pornography and other harmful content. Particular sites such as the web forum of the Free Azerbaijani Movement (http://www.azdiaspora.org), created by an Azerbaijani military officer, is not accessible through ISPs connected via Delta Telecom, while those connected via Azertelecom allow access to the site, according to Expression Online. In times of crisis some media sources have been blocked.

However, the first known instance of the blocking of a site that hosts content beyond that of a justifiably-threatening nature has occurred. In January 2012, 1.7GB of internal documents from the Special State Protection Service of Azerbaijan were leaked by the Anonymous organization. Documents that were deemed interesting by Anonymous were also uploaded to the image sharing site Imgur.com. Imgur.com is a popular site for anonymous hosting of images, especially for the website Reddit. Soon after the release, Azerbaijani Internet users were unable to access any images hosting on Imgur.com. As of August 2013, Imgur was still inaccessible in Azerbaijan. Overall, the technology for filtering exists, the Azerbaijani government has used it in the past, recently has used it on a site that is not exclusively a security risk, and public rhetoric has suggested that the government has considered filtering Facebook.

Facebook is a particular threat to the Azerbaijani government. After an increase in Facebook activism in early 2013, some pro-government Azerbaijani politicians made statements about limiting or blocking Facebook. “These networks create a threat to Azerbaijan’s statehood” Fazail Agamali, leader of the pro-government party Motherland said to

---

49 Deibert and Rohozinski. 2010. “Control and Subversion in Russian Cyberspace.”
52 http://par-anoia.net/releases2013.html#dmx
53 http://imgur.com/a/cylKb#0
54 http://advocacy.globalvoicesonline.org/2013/02/07/imgur-com-blocked-in-azerbaijan/
Social Media in Azerbaijan

Turan on March 11, 2013\(^{55}\) and other news outlets.\(^{56}\) The government quickly responded to this statement that it was not planning on blocking Facebook,\(^{57}\) but that was not the last mention of Facebook as a threat. Azerbaijan’s Interior Minister Ramil Usubov also criticized Facebook on March 13, 2013.\(^{58}\) And the Azerbaijani National Security Minister Eldar Mahmudov linked Facebook in Azerbaijan to international terrorist rings at the International Conference on Strengthening Cooperation in Preventing Terrorism on March 18, 2013.\(^{59}\) On April 2, 2013, MP Hadi Radjabli, Chairman of the Permanent Committee for Social Policy of the Azerbaijani Parliament, attacked Facebook as a bad influence and suggested that social media should have more pro-government content.\(^{60}\) While these assaults on Facebook are not filtering, per se, the public discussion of Facebook as a threat to security implies that the government has considered filtering Facebook.

**Policing cybercafés**

While there is no widespread policing of cybercafés, there is some evidence that they are targeted,\(^{61}\) and some claims about the danger of cybercafés for children. The Azerbaijani State Committee for Family, Women and Children’s Affairs “has conducted monitoring in Internet cafes to examine the situation in this area. The results showed that children were going to “Internet clubs” during lessons and visit websites with negative impact.”\(^{62}\) This experimentation with monitoring cybercafés is an example of experimentation with monitoring as well as framing the monitoring as for the protection of children.

**Second Generation**

Second-generation Internet controls “create a legal and normative environment and technical capabilities that enable state actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery.” These controls are both overt and covert. Overtly, there is a legal infrastructure to control access to content. For example, concerns about cybersecurity and extending slander and defamation laws to the online space are evoked to create policies about Internet

\(^{55}\) http://www.contact.az/docs/2013/Politics/031100031350en.htm#.UYfz38p49ks

\(^{56}\) http://gunxeber.com/?p=60815

\(^{57}\) http://news.lent.az/news/119078

\(^{58}\) http://en.apa.az/news/189340


\(^{60}\) http://www.haqqin.az/news/4775


\(^{62}\) http://www.azernews.az/azerbaijan/46785.html
control. Covertly, procedures and technologies are deployed to control access at times of crisis.63

**Overt**

Telecommunications law in Azerbaijan was created in 2005, but does not cover access to content. However, in June 2012, the Azerbaijan criminal code was amended to reflect the Council of Europe’s Convention on Cybercrime that it signed in 2008. The amendments are fairly standard regarding data integrity and preventing the use of computers for criminal purposes.64

Until April 2013, online and offline content was regulated by the same set of laws, as the Internet is considered part of the mass media65. Of particular interest are Azerbaijan’s criminal and civil defamation laws, which are quite broad.66 On April 30, 2013, however, the Azerbaijani parliament introduced amendments to the criminal code that would specify the Internet (including both media websites and personal social networking sites) in defamation and libel laws67 and on May 14 the law passed.68 Azerbaijan’s minister for Communication and Information Technology supported the amendments in statements on May 6, 201369 and President Aliyev signed the online defamation law on June 6, 2013.70 The first criminal online defamation case occurred in the fall of 2013, when a former employee of a regional Azerbaijani bank was accused of defaming his former employer by creating a Facebook page about that bank being unfair and corrupt. (Notably only 26 Facebook users “liked” the page, implying that it did not have a wide reach.) He was sentenced to one year public work and 20 percent of his monthly salary will be withheld for a year.71

Moreover, publicizing opinions that instigate extremism or have “harmful content” is illegal, as per Articles 214-216 of the Criminal Code.72 In May 2011, officials claimed that spreading misinformation is a...

---

63 Deibert and Rohozinski. 2010. “Control and Subversion in Russian Cyberspace.”
64 http://president.az/articles/5426
68 http://www.contact.az/docs/2013/Politics/051400036136en.htm#.UZJoVspXrDt; http://en.apa.az/news_azerbaijan_sets_punishments_for_internet_192821.html
70 http://www.rferl.org/content/azerbaijan-internet-defamation-law-criminal-aliyev/25008799.html
cybercrime and noted Skype and Wikipedia as threats to national security.\textsuperscript{73}

**Covert**

Internet Service Providers in Azerbaijan legally can cut Internet service under broad circumstances and during war, emergency situations, or natural disasters, an Internet kill switch can be activated.\textsuperscript{74} Also, distributed denial of service (DDoS) attacks, which can overwhelm an Internet website host, effectively taking down the site, can be ordered by anyone.\textsuperscript{75} There are some claims that attacks are ordered by the Azerbaijani government.\textsuperscript{76} And in particular, a DDoS attack on an opposition newspaper is claimed to have originated at the Azerbaijani Ministry of Communications and Information Technologies.\textsuperscript{77}

**Third Generation**

Third generation controls are more sophisticated and multidimensional. Third generational controls compete with potential threats through effecting cognitive change rather than deny access.\textsuperscript{78} Deibert and Rohozinski focus on three types of third-generation controls: surveillance, state-sponsored information campaigns, and direct action. This paper will elaborate on the state-sponsored information campaigns with a focus on trolling. Trolling has four sub-categories: memes, Twitter shenanigans, blocking, and Kompromat. This is also where the individuals and organizations within the Azerbaijani government hierarchy begin to emerge.

**Surveillance**

While there is evidence that the Azerbaijani government does engage in online surveillance, there is a widespread belief that the government does monitor citizens offline and online, and this impacts people’s behavior online. A report by Swedish investigative news show *Uppdrag Granskning* found that the Swedish telecommunications company Teliasonera (amongst others) has sold surveillance equipment to the Azerbaijani government.\textsuperscript{79} “Black boxes” or “black rooms” are installed in the server rooms of mobile telecommunications companies and Internet service providers.\textsuperscript{80} There is also substantial anecdotal evidence of surveillance. Azerbaijani activists

\textsuperscript{73} http://www.eurasianet.org/node/63554
\textsuperscript{74} Expression Online. 2012. “Searching for Freedom: Online Expression in Azerbaijan.”
\textsuperscript{75} Deibert and Rohozinski. 2010. “Control and Subversion in Russian Cyberspace.”
\textsuperscript{76} http://www.irfs.org/news-feed/azerbaijani-government-sparks-an-open-season-on-critical-websites-amid-pre-election-crackdown/
\textsuperscript{77} http://www.indexoncensorship.org/2012/11/azerbaijan-internet-freedom/
\textsuperscript{78} Deibert and Rohozinski. 2010. “Control and Subversion in Russian Cyberspace.”
\textsuperscript{79} https://www.eff.org/deeplinks/2012/05/swedish-telcom-giant-teliasonera-caught-helping-authoritarian-regimes-spy-its
\textsuperscript{80} Expression Online. 2012. “Searching for Freedom: Online Expression in Azerbaijan.”
report having printed Facebook private messaging transcripts handed to them while in police custody. Others have seen logins from multiple IP addresses in Facebook and Gmail.

In March 2013, a number of opposition youth activists from the group N!DA (Exclamation in Azerbaijani) were arrested and were directly accused of using Facebook for illegal activity – which they deny. On March 8, 2013 the Ministry of National Security and the Chief Prosecutors office issued a statement that the three activists, Bakhtiyar Gulyiyev, Shahin Novruzlu, and Mahammad Azizov, were detained because they were on Facebook calling for violent forms of protest and were actively discussing the preparation and use of smoke grenades and Molotov cocktails in a street rally. Reportedly, the authorities found 23 Molotov cocktails; approximately $100,000 in cash; 507.67 grams of hashish; and 190.02 grams of marijuana in the homes of the activists, although they and their parents are adamant that the drugs and cocktails were planted and have excuses for the amount of cash in the homes. Notably, some of these young men were also administrators of an anti-government parody Facebook page.

It is difficult to determine if the surveillance activities described above are automated, such as the black boxes, or human. However, there is speculation that police departments pay young people to monitor Facebook and report opposition activities.

State-Sponsored Information Campaigns
Over the past few years, the Azerbaijani government has waged an aggressive media campaign against social media. Television programs show “family tragedies” and “criminal incidents” after young people join Facebook and Twitter. In March 2011, the country’s chief psychiatrist proclaimed that social media users suffer mental disorders and cannot maintain relationships. In April 2012, the Interior Ministry linked Facebook use with trafficking of women and sexual abuse of children. An April 2013 story mentioned drug and alcohol addictions, jealousy, suicide, and the destruction of friendships and families related to social media use.

82 http://elitar.az/nida-cilar-hayd%C9%99r-%C9%99liyev-adina-s%C9%99hif%C9%99-yaratdiqlari-ucun-h%C9%99bs-olunub/
83 http://bizimyolinfo.com/?sehife=1&xeber=9314#.UWm4Jjoo7Zp.facebook
In May 2013, the Minister of Communication and Information Technology stated that Facebook causes divorce.\(^{88}\)

This sort of framing of social media as dangerous may not deter all Azerbaijanis from using these services, but it certainly helps the government do two things: first, keep a portion of the population away from social media\(^{89}\) and, second, sets the stage for these sites being dangerous in case it chooses to block them in the future.

**Trolling**

While there is little academic research on the phenomenon of trolling, it can be understood as the “posting of incendiary comments with the intent of provoking others into conflict”\(^{90}\) and a *troller* is a computer-mediated communication user who has the intention of causing disruption and/or triggering or exacerbating conflict for the purpose of their own amusement.\(^{91}\) Similarly, Rafferty defines trolling as “the attempt to hurt, humiliate, annoy, or provoke in order to elicit an emotional response for one’s own enjoyment.”\(^{92}\) And Bergstrom defines trolling as the transgression of community norms that results in anger, harm, or discomfort. Trolling differs from teasing in its intensity and level of mercilessness.\(^{93}\) Phillips gives a particularly cruel example of trolling where individuals make jokes on Facebook memorial pages of the recently deceased.\(^{94}\) As McCosker argues, trolling is a complex set of practices, and thus, in the author’s estimation, is difficult to define in an all-encompassing way.\(^{95}\) As such, this article will describe some types of trolling in Azerbaijan to better understand the set of practices. Although all of these definitions acknowledge that trolling is by nature antagonistic, it is important to note that, as Milner argues, trolling is a communicative tool that can be used.

---

\(^{88}\) http://en.trend.az/capital/business/2147219.html

\(^{89}\) Pearce and Kendzior. 2012. “Networked Authoritarianism and Social Media in Azerbaijan.”


to diverse ends and serve multiple purposes.\textsuperscript{96} Thus, there can be other goals of trolling, as we see in Azerbaijan, such as control or deterrence of expression or dissent. A revised and expanded definition then could be that trolling is the creation of (with intent to share) and sharing of digital content by individuals or groups with the intent to antagonize, provoke, harm, humiliate, or control other individuals or groups.

Four types of this provocative and conflict-generating trolling in Azerbaijan are memes, blocking, shenanigans on Twitter, and Kompromat. Memes, shenanigans, and blocks seem to be mostly conducted by the pro-government youth organizations, while Kompromat is not attributed to the pro-government youth organizations, the resources put into it are evidence for in-direct government involvement.

**Memes**

Pro-government forces in Azerbaijan to humiliate oppositionists commonly use Memes. A more detailed discussion of memes is included in the article by Pearce and Hajizada in this issue, and thus will not be discussed here.

**Blocking**

Another technique that the government and its allies use is filing complaints with Internet services about users that it wishes to silence. This can be done with a specific post or a user’s profile overall.

The example in Figure 1 is a boasting post where a pro-government youth group chairman shows how he reported the well-known opposition journalist Khadija Ismayilova’s Facebook post for “harassment.”

**Figure 1. A blocking action by a pro-government activist secured the removal of a post by an opposition journalist.**

Although the systems for reporting harassment are designed to protect users, in Azerbaijan it is not uncommon for social media users affiliated with the opposition to find themselves blocked from the service with little recourse. For example, Facebook users may find themselves accused of posting something that violates Facebook’s policies and being blocked from using similar features for 24 hours or more.

Facebook has means for becoming “unblocked” but the steps involved are difficult, especially for those not fluent enough in English to read through the legalese-laden terms of service and community standards. Reasons for blocking may be viewed as “technicalities” like copyright infringement by those whom are blocked, but for Facebook, these are serious issues and are possibly best dealt with through a strict policy. Thus, when a blocked individual attempts to argue for being unblocked because of political motivations on the part of those who filed the original complaint, it is difficult for Facebook to deal with these individual cases and have to make exceptions to its own policies.

Twitter Shenanigans
While Twitter is not nearly as popular in Azerbaijan as Facebook is (as is the case globally), some elite users do engage with it. While Twitter posts often mirror Facebook posts (for both individuals and organizations), one difference is that analytics are readily available. The ability to measure social media reach is attractive to some Azerbaijani social media users.

Hashtags are keywords to organize information to describe a tweet and aid in searching.\(^\text{97}\) When a hashtag “trends” – it is noted by Twitter as being popular at a particular time. Users want a hashtag to trend to gain visibility and attention. While occasionally hashtags trend organically, it is much more common that hashtags are artificially pushed to the trending list.\(^\text{98}\)

The pro-government youth group is particularly boastful about the number of tweets that its sponsored hashtags receive by “winning” with the largest percentage of Twitter posts. The interest in having metrics for and “winning” hashtags has caused this group to engage in Twitter shenanigans in four ways: hashtag creation, hashtag hijacking, zombie tweets, and mimicking profiles.

Hashtag creation
The pro-government youth group members create hashtags to troll and attack particular individuals. Opposition journalist Khadija Ismayliova


was the victim of “Shame on Khadija” #khadijautan.99 The pro-government youth group chairman proudly displayed the large reach that the anti-Ismayilova hashtag and that a hashtag campaign against an opposition youth group, N!DA, had, according to their analytics (see Figure 2).

Figure 2. Analytics for a Hashtag creation campaign.

Hashtags attacking the detained N!DA members and asking Ruslan Asad about his military service (described in the article by Pearce and Hajizada, this issue) were created and similarly celebrated.

Hashtag hijacking
When a hashtag is proposed for an event or topic, the intention is for a community of users to share information with each other. When a hashtag is hijacked, a group of individuals “take over” a hashtag by posting messages unrelated to the “spirit” of the hashtag as an information resource and conversation. For example, #armvote13 was about reports of election violations and election results, and people were using it to write things against Armenia and Armenians. The pro-government youth group engaged in hashtag hijacking for all of the 2013 protests,100 and election in Azerbaijan,101 as well as two hashtags of interest to Armenians, #armvote13102, and #armeniangenocide,103 to varying degrees of success.

99 http://www.katypearce.net/khadijautan-update/
100 http://www.katypearce.net/protestbaku-now-that-the-weekend-is-over-what-happened/
101 http://www.katypearce.net/shenanagins-again-and-again/
102 http://www.katypearce.net/armvote13-hashtag-got-taken-over-looks-suspicious/
103 http://www.katypearce.net/why-is-it-impossible-to-hijack-armeniangenocide-on-twitter-
By taking over hashtags, the pro-government youth groups can destroy the affordances that Twitter provides. For example, during a protest Twitter can serve promotional purposes, give locationally situated information (such as police presence), and allow for live reporting. Hijacking damages these affordances and takes the alleged power of social media back. Thus, this is another example of controlling information flow as a tool.

**Zombie tweets**

To get high numbers of users on a hashtag or hijack an existing hashtag, the pro-government youth group has had to coordinate its members to use the hashtag and tweet on it. First, it appears that the pro-government youth group members are either directed to tweet statements or, more likely, that someone at the pro-government youth group has control (password access) of members’ Twitter accounts. In the images reproduced in Figure 3, you can see that the same text was posted on Twitter by multiple accounts, only a few minutes apart or even at the exact same time. This is indicative of a Twitter client or service that allows for massive posting from multiple accounts nearly simultaneously. (Tweets in gray are exact duplicates). This differs from “retweeting”, where a message is intentionally duplicated, but with attribution to the original.

The second technique that the pro-government youth group uses is to create or purchase fake Twitter accounts (not an uncommon practice globally) to both tweet messages on a particular hashtag and to “follow” the pro-government youth group users in order to make it appear that they have a larger audience than they actually have.

---


Figure 3 Evidence of zombie tweets.

Figure 4 tracks the pro-government youth group’s chairman’s personal Twitter account. On the day before April 24, Armenian Genocide Memorial Day, his Twitter followers tripled.
Figure 4. Evidence of an artificial increase in the number of followers

An analysis of his followers (see Figure 5) showed that the majority are obviously fake accounts. Normally Twitter users have written at least one tweet and follow some people. Furthermore, no native English speaker would write his or her location as CANADA, Regina or USA, Connecticut. (The second column is number of followers, the third is number of tweets.)

Created accounts are also common. In an analysis of the October 2013 Azerbaijani presidential election hashtag, created accounts were found. In February 2013, hundreds of accounts were created within minutes of each other. These accounts were tweeting the same messages at the exact same time. Moreover, a reverse image search of the profile photographs of these created users determined that the images were found to be freely available on the Internet and used on dozens of different websites, associated with multiple countries and names.106

Mimicking profiles
Perhaps the most creative Twitter shenanigans that the Azerbaijani government and its allies has engaged in is creating Twitter profiles that mimic the profiles of some of the most popular opposition Twitter users.

106 http://www.katypearce.net/shenanagins-again-and-again/
During the March 10 protest, opposition activists Emin Milli, with the Twitter username of @eminmilli and Adnan Hajizada, with the Twitter username of @fuserlimon, were tweeting posts with the hashtag #protest-baku, retweeting Twitter posts from their friends, and writing @replies to other users. After a few hours and some tweets from both of these men that seemed odd, other Twitter users realized that the accounts were not Milli and Hajizada, but rather mimicking accounts with @eminmilli and @fuserlimon. (Both with significantly fewer followers than the men’s real Twitter accounts have.) However, with the exact photographs in their Twitter profiles and only one letter different, it was easy to fool others (See Figure 6).
Figure 6. A fake Twitter Account

Emin Milli
@eminmilli
I am dissident writer living in Azerbaijan. Baku, Azerbaijan - eminnlli.posterous.com

78 TWEETS 374 FOLLOWING 23 FOLLOWERS

Tweets

Emin Milli @eminmilli
@GulselSafarova Siz anlayanda gec olacag xanim!
View conversation

Emin Milli @eminmilli
@niyazi @baqani @RaufMardiyev Tarbiyaniz ele buna catur!
Hayat yoldaşim arasında meydanda idi. Digerlerinin hayat yoldaşlanda fırıl!
View conversation

Emin Milli @eminmilli
@EFatullayev Турсун как обычно пользуется доверчивостью читателей! К сожалению! #protestbaku
View conversation

Emin Milli @eminmilli
@GulselSafarova Xanım yamilsiniz! Sahlınızı anlayandacox gec olacag! #protestbaku
View conversation

Emin Milli @eminmilli
@baqani Bize hec bir şey eda belmayacaksiniz! @RaufMardiyev #protestbaku
View conversation

Emin Milli @eminmilli
@QanUral @namnikamal hamin gob rəxətə bərəxən tənəyyərm. Cox eglədi gəncərlər idil! Əsl NIDA-çılar idilər! #protestbaku
View conversation

Katy Pearce @katy_pearce
Caucasus aren’t giving me a break today.
Retweeted by Emin Milli
Expand
Kompromat
Kompromat, meaning “compromising material” or “blackmail files,” “refers to discrediting information that can be collected, stored, traded, or used strategically across all domains: political, electoral, legal, professional, judicial, media, or business.” Kompromat can be character assassination, blackmail, and manipulation of public opinion. Today it usually implies unsubstantiated or unproven damaging information. Szilagyi further defines kompromat as information with intent to denounce, expose, unmask, slander, destroy, or neutralize. Kompromat functions as a commodity for mass consumption, as a weapon to destroy opponents, and for bargaining and blackmail. Ledeneva finds that about 90% of kompromat is perceived as fabricated, yet it remains a popular political technique.

Ledeneva’s typology of kompromat includes political, economic, criminal, and private.

Political kompromat consists of political activities such as abuse of power, relationships with oligarchs, or political disloyalty. Economic kompromat includes misappropriation of budget funds, embezzlement, and bribery. Criminal kompromat includes ties to organized crime, contract violence and killings, and spying. Private kompromat includes illegal income, sexual behavior and orientation, unpopular ideologies, and family member misbehavior. Private kompromat, according to Ledeneva, is the most effective because of the strong social prejudice against these activities.

Kompromat is nothing new in Azerbaijan, but the Internet provides an effective and fast channel for kompromat dissemination. While kompromat has been disseminated in various ways, in late April 2013, the website http://www.ictimaipalatka.com/ and in early May 2013, http://www.gelherekati.com opened with the exclusive task of kompromat dissemination. Registered under a seemingly fake name for Ictimai Palataka and with a privacy service for Gel Here Kati, these sites are updated multiple times a day with videos, photographs, and cartoons, many of a sexual nature, featuring opposition members. The production quality is very high. The “sex tape” videos appear to be either coincidental lookalikes or hired lookalikes. The photographs appear to be photoshopped, but look fairly professional.

108 Ledeneva. 2006. How Russia Really Works..
Impact of Government Control of the Internet

The Azerbaijani government effectively controls the Internet by focusing on second and third generation means of control. By using psychological techniques as well as selectively punishing online dissent, it creates an environment of self-censorship. By not engaging in a great deal of first generation controls, the government can claim that it is not blocking access to content. Yet, second and third generation controls are likely more effective because of the psychological effect and creation of a self-censoring user base. Trolling is a particularly effective means of controlling and deterring dissent in Azerbaijan, in part because there is little that a target can do about it. The government’s co-opting of some of the social media strategies of the opposition may continue beyond memes and trolling. While GONGO’s have less need for fundraising than opposition groups do, activities like the pro-government youth group’s social media academy\textsuperscript{110} demonstrate that there is increased interest in using social media. And certainly, as Internet penetration grows in Azerbaijan, opportunities for citizens to demonstrate their loyalty online will continue.

Currently the psychological techniques and selective punishment are working in the Azerbaijani government’s favor. However, if Internet use continues to grow, it may need to increase either the quantity or type of those punished or deepen the punishments. While the “Donkey Blogger” case possibly had a slight negative impact on the global public opinion of Azerbaijan, it did little to deter the government from further punishment of online dissent. With the adoption of the new online defamation law, there may be no need for a “cover story” of hooliganism or drug use because the online action itself can be punished. It remains to be seen if this new law will increase sentences for online actions, but certainly it provide an easier path for taking such action.

Conclusion

Azerbaijan is a unique case for understanding the political use of the Internet because, while it is the primary space that the opposition has to disseminate information (to varying degrees of success), the government responds with a multilevel system of control, with a particular focus on effective psychological means of control. This article is not meant to be a case study of the failure of the Internet as a tool for democratization, but rather points out that, as Oates argues, “[U]nderstanding how particular nations harness the power of the Internet illuminates how national power can limit the international potential of a communications technology.”\textsuperscript{111}


It is important to note that the third generation tools of control used by the government are often focused on those engaged in connective action. It is possible that these new action networks are more difficult, even frustrating, for the Azerbaijani government to deal with. The government knows how to understand the traditional opposition parties and has an infrastructure for managing the opposition. With connective action-enabled networks, there is much greater uncertainty about motivations, behaviors, activities, and future prospects. It is perhaps because of this that the government has become increasingly heavy handed in its control of the digital space – including offline punishments for online activities.

The existing and likely growing potential for conflict between the traditional opposition organizations and the connective action organizations could provide an opportunity for the government to exploit these divisions and further fracture the opposition and weaken all the groups.