tripleC 14(2): 496–515, 2016
http://www.triple-c.at

When States Strike Back: Failures of Mediatized Activism in Azerbaijan and Turkey

Ilkin Mehrabov

Karlstad University, Department of Geography, Media and Communication Studies, Karlstad, Sweden, ilkin.mehrabov@kau.se

Abstract: This article is an empirically grounded conceptual investigation of the failures of mediatized activism in 2011 in Azerbaijan and Turkey. By analyzing two specific cases, namely the complete dispersion of corporate social media based opposition in Azerbaijan, and arrests of Anonymous led hacktivists in Turkey, the article aims to contribute to the discussion on the future of mediatized activism in the face of the growing pervasive surveillance, conducted by state intelligence agencies in collaboration with private infotainment and telecommunications companies. By elaborating on the shortcomings and the promises of social media based activism and hacktivism, the article discusses the possibility of building alternative online spaces, which can bring these two types of mediatized activism together, and help to connect activists with the rest of the society—especially the otherwise consenting middle classes of semi-authoritarian countries.

Keywords: Azerbaijan, Hacktivism, Social Media Activism, Surveillance, Turkey

Acknowledgement: The author thanks Dr. Miyase Christensen, Reinhard Handler and Raul Ferrer Conill for their extensive comments on the early draft of the manuscript; as well as the journal's anonymous reviewers for their concrete suggestions and constructive feedback

1. Introduction

Azerbaijan and Turkey, despite a number of key differences related to their size and history, share a set of striking similarities, especially when it comes to the events of the last decade. Besides being ethnic, linguistic, religious, and cultural cousins, both countries have gone through similar major transformations starting from 2003; experienced growing authoritarianism throughout the past decade; and witnessed consecutive political elections, not leading to any significant change.

Thus, as was the case all around the world, Azerbaijani and Turkish oppositional political movements were also influenced by the uprisings of 2011, and tried to conduct a series of "Arab Spring" inspired protests. However, the events following these attempts, throughout the time period of 2011–2015 in Turkey and Azerbaijan, served to highlight the fact that technically savvy states, and their surveillance capacities, are also continuously developing in reaction to increasingly mediatized nature of political activism.

Friedrich Krotz defines mediatization as a metaprocess—a long-term, historical process in (and through) which different forms of media emerge and are institutionalized (2009, 24). For him, mediatization is closely intertwined with three other important processes—globalization, individualization, and commercialization. He describes these four processes as the "relevant metaprocesses that influence democracy and society, culture, politics and other conditions of life over the longer term" (Krotz 2007, 257).

In line with the definitions of Krotz, in this paper I refer to the mediatized activism as a very specific case of online activism, which in itself is just one part of a broader category of mediated activism (Krotz 2009, 24). Thus, I define mediatized activism as a type of activism which is conducted exclusively through the online communication channels and with the help of the networked digital media technologies—over which activists, especially in the context of semi-authoritarian countries, most of the time have no (or very little) control.

Date of Acceptance: 10 October 2016
Date of Publication: 4 December 2016

Within this scope, this article is an empirically grounded conceptual investigation of the failures of mediatized activism in Azerbaijan and Turkey. Through the analysis of two specific cases, namely the complete dispersion of commercial social media based oppositional activists in Azerbaijan, and arrests of Anonymous led hacktivists in Turkey, I aim to contribute to the discussion on the future of mediatized activism in the face of the growing pervasive surveillance, conducted by state intelligence agencies in collaboration with private infotainment and telecommunications companies (Mattoni and Treré 2014; Tai 2015; Uldam 2016).

In order to attend to the research aim specified above, in the Azerbaijani case, the *Global Digital Activism Data Set*, developed by the Digital Activism Research Project of the University of Washington, was used as a starting point. I then integrated into this set the information obtained from the detailed yearly reports of *Human Rights Watch*, *Amnesty International*, and *Freedom House*, thus forming a database with details of all the online and offline protests, which took place in Azerbaijan between 2003 and 2015. This data source was combined with thorough searches I conducted in the online newspaper archives of *Azadlıq Radiosu*, *Radio Free Europe/Radio Liberty* and *Yeni Müsavat* in Russian, Azerbaijani and English languages. This constituted database is not unique to this article, and was used for other studies as well (Mehrabov 2015b; Mehrabov 2016).

Two humorous Facebook groups, *HamamTimes*[1] and *AzTVdən Seçmələr*[2] are among the strongest critiques of the ruling government in Azerbaijan, and frequently update their pages with posts about Azerbaijani protests. Although both of the groups were formed in 2012, they have posts about the past demonstrations as well: in the form of circulated images and videos, calls for action, opinion pieces and status updates of opposition leaders and key activists. Thus, I closely followed both the current feed of these groups, as well as their archived posts, where some of the updates had generated hundreds of online comments.

For the Turkish case I benefited from the written notes I took while attending *Surveillance, Censorship and Data Protection in Turkey* panel of ECREA's pre-conference *Imposing Freedoms*, organized in Istanbul on 23 October 2012. The protests against Internet censorship, as well as Anonymous attacks of 2011, were among the main topics of presentations at the session, as well as of the informal discussions I chanced to have with the presenters and the audience members—Turkish academics, activists and representatives of various NGOs.

I further compared these notes against the massive debate page, stored on the website of Alternative Informatics Association (Alternatif Bilişim Derneği),[3] Turkish civil society organization focused on the issues of Internet censorship and mass surveillance; the selected period (May 1–June 30, 2011) of #OpTurkey hashtag's feed on Twitter; and archives of now defunct Facebook groups: *İnternetime Dokunma*[4], established as the communication medium for the participants of 15 May demonstrations against the Internet filter, and *Internetime Dokunma—Sharpies Revolt*[5], founded on 18 May 2011 as the main collaboration platform for dissemination of these protests' international news coverage.

Integrating all these information sources, I firstly look into and analyze how events unfolded in Azerbaijan and Turkey. Based on this evaluation, I engage into a discussion of factors, (probably) contributing into the failures of Azerbaijani and Turkish mediatized activisms. Later I reflect on promises and shortcomings of social media based activism and hacktivism, and in the end theorize on a formation of an alternative online platform, which can (possibly) bring these two forms of mediatized activism together, and help them in reinforcing each other in a complementary manner.

I argue that the proposed alternative—by helping activists to reconnect with the rest of the society, especially the otherwise consenting middle classes—can especially be valuable in the context of semi-authoritarian countries, where governing regimes are in complete control over Internet infrastructure and are closely monitoring commercial social media.

[1] https://www.facebook.com/HamamTimes/
[2] https://www.facebook.com/pazaztv/
[3] https://www.alternatifbilisim.org/wiki/Ana_Sayfa
[4] https://www.facebook.com/15mayis/
[5] https://www.facebook.com/sharpiesrevolt/

2. Social Media-Based Activism in Azerbaijan

The turbulent "Arab Spring", blustering across the Middle East, inspired a renewed insurgent oppositional spirit to find voice also in Azerbaijan. Especially in March and April of 2011, Baku witnessed a few demonstrations, where hundreds of activists took to the streets to protest against government corruption, to call for fair elections, and to demand respect for human rights (Freedom House 2012, 59). Admittedly inspired by the riots in Egypt and Tunisia, young oppositional demonstrators used commercial social media platforms to reach out to wider audiences and to call for organized cycles of rallies (Amnesty International 2011b, 16).

These offline protests led only to the further deterioration of an already diminished freedom of assembly, as state officials did not permit any gatherings and police and other law enforcement agencies quickly, and quite often very violently, dispersed unauthorized demonstrations (Human Rights Watch 2012, 419).

In the meantime, corporate social media-based calls for action, especially those launched on Facebook, mostly resulted in activists being arrested within a matter of days, if not hours, after placing their posts online. Since oppositional activists who used social networking sites to call for protests and express their displease with the government were always on the lookout for the novel ways of opinion expressing and information exchange, police forces heavily cracked down on all forms of online dissent through the series of interrogations, detainments and imprisonments of key organizers and activist leaders (Amnesty International 2011b, 21).

The earliest and one of the most prominent of such cases was that of Jabbar Savalan, a student member of oppositional Azerbaijan Popular Front Party, who updated his Facebook profile with a call for a "Day of Rage" at Baku's Azadlıq Meydanı (Azadliq Square). He made the Facebook post on 4 February 2011, but immediately the next day, on February 5, he was detained by police (Amnesty International 2011a, 1). Events unfolded in a similar manner in the second case as well. On 4 March 2011, oppositional activist Bakhtiyar Hajiyev was arrested. He was a co-founder of Facebook group "calling for an 11 March virtual protest against government corruption and oppression" (Amnesty International 2011b, 23), and his arrest came only two days after the group was founded, and right after the page became publicly visible.

According to the assessment of Freedom House, access of Azerbaijani Internet users to online social media platforms such as Facebook and Twitter is unrestricted, and these websites are still being extensively used to criticize government policies. Among all of the available sites, especially Facebook had turned into a "key source of information on rallies, protests, and social issues such as housing demolitions" (Freedom House 2012, 57). Yet, looking back at their evaluation from the previous year, which states that it is "unclear to what extent security bodies track user data in Azerbaijan" (Freedom House 2011, 45), it becomes quite obvious that Facebook is now closely monitored, and quite possibly in a real time manner. Judging from the response rate of Azerbaijani law enforcement agencies to activists' Facebook posts, it could be said that the speed with which the government responds to cases of online dissent has dramatically improved. This is evident from a comparison of Facebook cases from 2011 with a YouTube case of 2009.

On 28 June 2009, activists and bloggers Adnan Hajizada and Emin Milli uploaded a video, which humorously featured a donkey delivering a fake press briefing, to YouTube. The video made fun of news about the government officials' spending of hundreds of thousands of US dollars to import a dozen donkeys from Germany, through a deal which allegedly was masking "corruption or theft of public funds" (Amnesty International 2011b, 9).

On 8 July 2009, the duo was attacked while dining. When they went to the police, events took an odd turn. Instead of their attackers, bloggers themselves were pressed with charges of hooliganism and on 11 November 2009, were sentenced to 30 and 24 months of imprisonment (Pearce and Hajizada 2014, 75). This incident drew international attention, as both national, as well as international human rights organizations believed that the bloggers were facing bogus charges, fabricated in response to their public criticism of the Azerbaijani government (Amnesty International 2011a, 3). This incident established Azerbaijan as one of the

pioneer countries in arresting activists for their use of Internet humor (Pearce and Hajizada 2014, 75).

Adnan Hajizada and Emin Milli were conditionally released in November 2010 after an international campaign was started on their behalf (Amnesty International 2011a, 3). The efforts of lobbying for their cause were undertaken by a number of human rights associations, non-governmental organizations and individuals all around the world, including prestigious entities such as Global Campaign for Free Expression, Human Rights Watch, ARTICLE 19 and International PEN (European Stability Initiative 2011, 22).

According to a *The New York Times* article, focusing on the case of Emin Milli after he was released from prison, he reportedly found out that all of his life had dramatically changed while he was serving his term. None of the organizations that used to employ him as a translator would use his language skills again, fearing to anger the Azerbaijani state officials. Because of Milli's dissident position his father-in-law was fired from his governmental post. His own father had died while Emin Milli was in prison, and Milli's wife had officially asked for a divorce, fearing for her own future (Barry 2011).

Both the arrest of the bloggers, and the later repercussions that followed, were widely reported on Azerbaijani news portals, discussed on online sites and shared on social media platforms. This wide publicity only resulted in a steep decline in support for mediatized activism, despite many young Azerbaijanis' sympathy for the bloggers and shared political beliefs with them. According to Katy Pearce and Sarah Kendzior this mainly happened due to the fact that by "publicizing the reprisals for even mild, humorous forms of dissent, the government provoked anxiety among Azerbaijanis insecure about the future and hesitant to engage in protest" (2012, 286–287). Emin Milli himself explained the occurring situation as

> I think this is the way they function […] They don't organize mass killings. They just do it this way. They punish some people and let everyone else watch. To say, 'This is what can happen to you' (Barry 2011).

In her study, critically interrogating the relationship between the Internet and democratization process in China, Rebecca MacKinnon introduces the concept of networked authoritarianism (2011). She defines a networked authoritarian state as a type of society where a wide range of discussions about the problems of a specific country occur on various websites and social media platforms, and people are even able to use the Internet portals to call attention to the different cases of injustices, social problems, corruption and malfeasances—while the single ruling party continues to remain in the complete control of online infrastructure and the government agencies closely follow and monitor this chatter, only occasionally censoring and manipulating online conversations. Nevertheless, as a general outcome of this novel form of governance, an "average person with Internet or mobile access has a much greater sense of freedom—and may feel that he has the ability to speak and be heard—in ways that were not possible under classic authoritarianism" (MacKinnon 2011, 33).

Looking at the case of Emin Milli through the lens of networked authoritarianism, Pearce and Kendzior argue that the means employed by Azerbaijani state agencies against mediatized activism conducted through the social networking sites, as well as the increasing use of violence in the real life, serves the exact same purpose.

The main aim is to remind Internet users, frequenting oppositional portals, that there is no more difference between the realms of the online and the offline, and that both are controlled by the state (Pearce and Kendzior 2012, 288). A similar view is expressed by Vafa Guluzade as well, the former adviser to the late Azerbaijani president Heydar Aliyev, when she opines that the type of havoc which was brought upon Emin Milli allows the state to prevent troublesome trends to take off from the beginning—as she states, when "two bloggers are punished in this way, there will not be a third" (Barry 2011). Thus, the cases of Facebook activists of 2011, who called for street action and real-life protests in order to challenge the state power, and their subsequent arrests with "trumped up charges, not related to the participation in the protests" (Amnesty International 2011b, 6), served as a message to the rest of the public.

These arrests functioned as a warning for the ordinary population of the country, since states that employ networked authoritarianism do not directly censor online dissent. Instead, these states choose to allow dissent for a short while and to "compete with it, making an example out of online dissenters in order to affirm the futility of activism to a disillusioned public" (Pearce and Kendzior 2012, 284).

After making an example out of prominent social-media based activists of 2011, Azerbaijani state started to use more advanced (and more sinister) techniques to regulate and monitor the Internet and social networking sites. Through the uses of psychological persuasion techniques as well as the further occasional punishment of online dissent, state was able to create an atmosphere of self-censorship, where especially trolling is now used in an increasing manner. It is a very effective way to control and deter online forms of dissent, partly because that there is (practically) nothing targeted victim can do about the cases of trolling (Pearce 2014, 65).

Yet, when all these measures fail, the process of detainment on false pretenses, followed by an immediate arrest, is still employed by state law enforcement agencies, as can be seen in the case of Omar Mammadov, who was taken into custody on 24 January 2014 (Amnesty International 2014, 13–14). Mammadov is an active blogger, and used to be an administrator of satirical Facebook group *AzTVdən Seçmələr* (Selections from AzTV)—which currently has more than 100,000 followers and is considered to be one of the most critical, and humorous, commentators on the general state policies and the individual state officials in Azerbaijan.

It is not uncommon that the pressures, placed upon social media sites by the state agencies, are also accompanied with propaganda, coming from the local, government controlled television stations. AzTV, the national public service broadcaster frequently ridiculed for its absurdly one-sided reporting practices, is among these TV channels. State propaganda, broadcasted from local TV stations, demonizes social media platforms, as these channels ran defamation campaigns against social networking sites. The most frequent technique, employed in the process of this demonization, is interviewing internet experts, psychologists and bureaucrats, who argue that "online activities could have a detrimental effect on Azerbaijan's image and pose a threat to the country's security" (ARTICLE 19 2012, 36).

3. #OpTurkey and Hacktivism in Turkey

Starting almost immediately from the point of its enforcement in 2007, the controversial Law #5651 "Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting" (5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yaynlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun) was met with a harsh criticism in Turkey and a number of protests against it occurred since. The scope of practices this law was supposed to deter, by preventing access to online providers of these services, was an eclectic mix—partly due to reliance on another law article in defining what constitutes an Internet-based criminal activity. In the end, the compiled list included acts such as,

> the sexual abuse of children (Article 103), orienting reader to a suicidal activity (Article 84), facilitating the use or narcotic or stimulant substances (Article 190), obscenity (Article 226), prostitution (Article 227), providing a platform for gambling activities (Article 228) and supply of dangerous substances imperiling health care (Article 194) (Tunç 2013, 157).

Going into effect right after it was officially adopted Law #5651 was interpreted in a very subjective manner and led to bans of numerous websites. The number and range of online portals affected by the law were vast. Because of individual interpretations of the law, different judges all around Turkey issued warrants, banning access to entirety of the massy video sharing platforms YouTube and Vimeo, and the giant blogging portals WordPress and Blogger (instead of blocking individual videos and blogs, which were deemed as "inappropriate"); the Kurdish news agencies; the websites about evolution and atheism; and the LGBTT social networking sites (Harris 2015, 260).

These prohibitions were challenged through online petitions to stop the implementation of the law; the Internet attacks against the governmental agencies involved in its enforcement; and a harsh criticism on social media platforms of the law's subjective interpretations. When none of these virtual acts helped, a number of physical demonstrations happened as well.

The first of these offline protests took place in July 2010, when responding to a call for action, issued by the campaign for freedom of Internet expression, over 2,000 people marched down Istanbul's Istiklal Avenue (Reporters without Borders 2011, 95).

So, the debate over the freedom of online speech was already overheated, when, in early 2011, Turkey's Information and Communication Technologies Authority (Bilgi Teknolojileri ve İletişim Kurumu) announced its plan about the new Internet filter. This centralized online filtering system was planned to go into effect on 22 August 2011 and required "Internet users to install a filtering software on their computers in order to protect them (particularly minors), from any 'objectionable' content" (Reporters without Borders 2012, 70). The system was interpreted by many as a latent attempt for online censorship, and in response, tens of thousands in some 40 cities and towns around Turkey engaged in street protests against the new legislation on 15 May 2011.

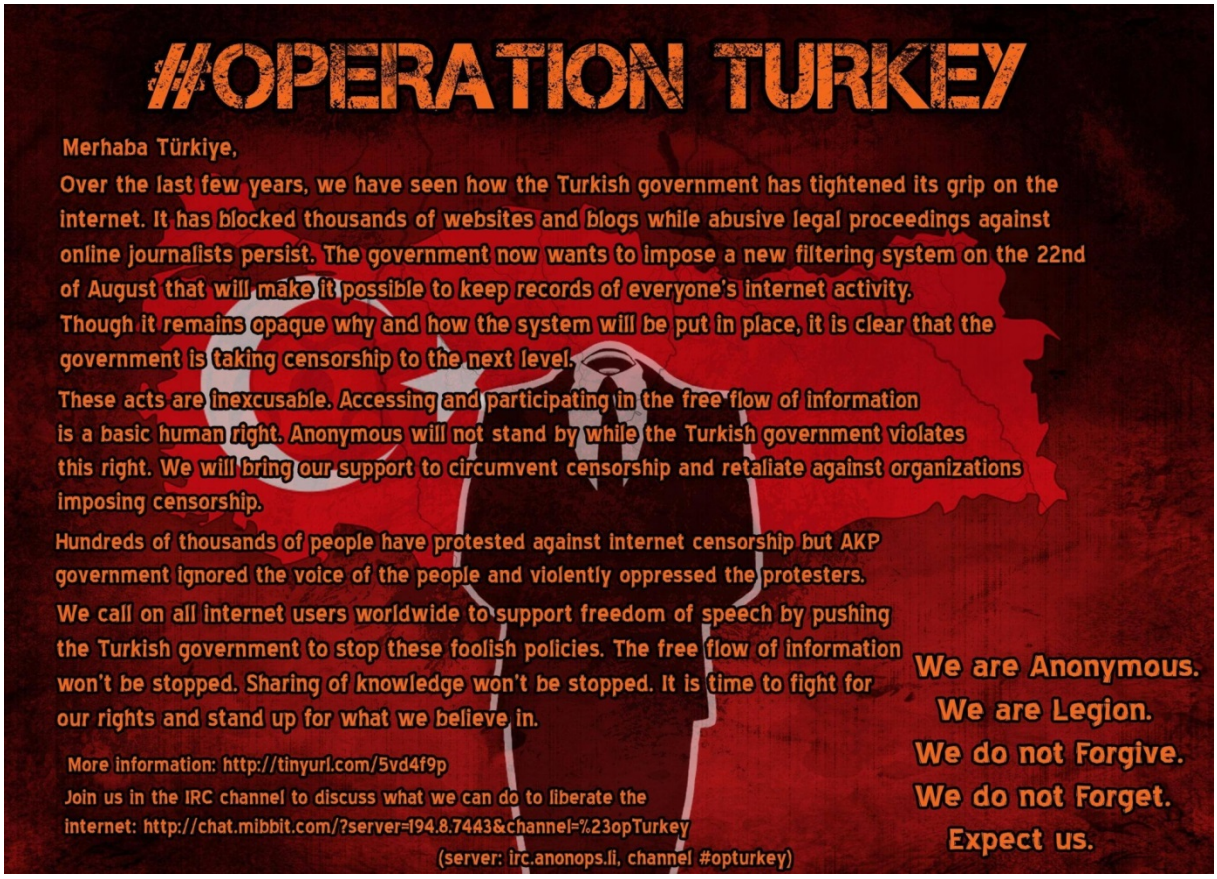

Figure 1: Anonymous' #OpTurkey Call.

It was under such circumstances that on 6 June 2011, the notorious hacktivist collective Anonymous announced its call for #OpTurkey, and invited everyone interested in the matter to participate in their Internet Relay Chat (IRC) discussions. "Operation Turkey" was designed as a series of coordinated service disruption attacks on the critical infrastructure and Internet service providers in the Turkish cyberspace and started on 8 June 2011. During the course of the next few days, many successful Distributed Denial-of-Service (DDoS) actions were launched, resulting in the block of Turkey's telecommunications authority's website, which was identified as the main target in the protest against the new online filtering system. Other governmental websites, including the social security services, meteorology, as well as

several telecoms-related portals were also affected. Ironically, one of the attacked sites was the official website where "people can report inappropriate Internet content" (Butler 2011). So it came as a great surprise when, on 12 June, only four days after the events started, 32 people, including eight minors, were arrested in 11 cities all around Turkey (Tremlett 2011).

The arrests of the individuals, allegedly connected to Anonymous' attacks on the governmental websites and charged with "illegally entering the communications system", happened through the synchronous raids of the Ankara police department's branch which otherwise deals with issues of smuggling and organized crime (Champion 2011). Although the response time of Turkish state was extremely quick, and came as a surprise to everyone, the upcoming incursion was actually hinted to the press before the raids started. A day before the raids, Turkish National Police announced that the staff of its Department for Combating Cyber Crimes, with the help of various cyber security experts from other state agencies, had compiled a list of (approximately) 250 suspects, believed to be involved in these attacks, and that they were gearing up for a massive operation against them (Şardan 2011).

The main reason behind the swift reaction of Turkish law enforcement agencies was that only few months before the Anonymous' attacks, in January 2011, Turkey conducted a cyber terror drill, which involved 39 Turkish national and private institutions, and aimed to coordinate the online response among these entities (Carr 2012, 261). Together with the important state cyber security agencies such as National Electronics and Cryptology Institute (UEKAE), Information and Communication Technologies Authority (BTK), Scientific and Technological Research Council of Turkey (TÜBİTAK), and Research Center for Advanced Technologies on Informatics and Information Security (BİLGEM), a number of private corporations such as the mobile services providers Turkcell, Vodafone and AVEA participated in the testing of the vulnerabilities of Turkey's online infrastructure—and significantly improved their capacities to deal with unexpected attacks on their information and communication systems (Hürriyet Daily News 2011).

4. Failures of Mediatized Activism

What connects these two (seemingly) separate cases from two different countries is that they both happened in 2011, in the heyday of Arab Spring inspired demonstrations all around the world; both heavily relied on media technologies; both were exclusively organized online; both tremendously suffered from the mediatized surveillance; both were unable to reach the necessary critical mass of mobilized people; and thus, in the end, both failed to achieve their main goals.

In the case of Azerbaijani demonstrations, forcing authorities to resign was stated as the main goal of the protests, with the devised shibboleth of "Azerbaijani People will show their rage against the dictatorial regime that has been squashing, humiliating, and violating their rights" (Geybullayeva 2011). Needless to say, this goal was not realized. On the contrary, the oppositional political movements got most of their key organizers and activist leaders arrested, while government was able to fortify its position—by adopting a "new law which dramatically increased the fines for organizing and participating in so-called unauthorized rallies" and heavily investing in anti-riot gears: water cannons, rubber bullets, tear gas capsules, and new Long Range Acoustic Device (LRAD) systems, the sonic weapons specifically developed for non-lethal crowd control (Bedford 2014, 9).

In the case of Turkish DDoS attacks, the Anonymous' #OpTurkey invitation was calling on all of Internet users worldwide to support the freedom of speech through pushing the Turkish government to stop the censorship policies (see Figure 1). Although the activation date of the announced Internet filtering system was postponed, the policy of blocking access to websites through the implementation of the Law #5651 continued. According to EngelliWeb[6], aggregator of statistics on the banned websites in Turkey, 113,664 websites[7] are currently inaccessible within the Turkish cyberspace.

[6] https://engelliweb.com/
[7] Last accessed on 1 October 2016—the number was 110,464 on 4 May 2016; and 80,118 on 17 May 2015.

So, even if commercial social-media based activism and hacktivism are practices that take different turns, by virtue of both being forms of mediatized activism they could be analyzed in a parallel manner. Such analysis not only helps to demystify their discourses, but also provides opportunities to discern limitations of mediatized activism within current socio-political configurations.

4.1. Commercial Social Media

The list of cases where governments (and not only the Azerbaijani one) easily monitored, watched, supervised; and, when they felt the necessity, arrested cyber activists with the help of logs of their social media use, calls for a scrutiny of social media platforms, especially the most popular ones such as Facebook and Twitter. Such an inquiry invokes further questions related with the current state of mediatized activism, conducted through these platforms, and the possible future(s) of online dissent. As Jillian C. York rightfully asks, why there is insistence on assigning commercial social media the role of the public sphere, while in reality social networking sites are "private ones, owned by billionaires and shareholders" (York 2014)?

In earlier Habermasian terms, public sphere was conceptualized as a space of interaction among citizens, who could openly discuss the common affairs with each other. Nancy Fraser questions commercial aspects of the public sphere, by emphasizing that ideally it should not be an "arena of market relations but rather one of discursive relations, a theater for debating and deliberating rather than for buying and selling" (Fraser 1992, 110)—yet, the distinction between the public-private loses its clarity on a commercial social media platform such as Facebook. Facebook's economic model for surplus generation is based on commodification of data, obtained from user interactions. This processed data is later on sold to advertising agencies and information brokerage companies, thus enabling Facebook to commodify "private data that is used for public communication in order to accumulate capital that is privately-owned" (Fuchs 2012, 147).

Such an economic model requires constant monitoring of users and keeping logs of every page they are following; every group they are member of; every article they liked; every post they commented upon; every link they shared; and every status update they posted. In this sense, every participatory act on Facebook is not an act of discursive interaction, but rather an information piece, which is used in order to monetize on user's meta-data. This is the case with other for-profit social media platforms as well, as in a quid pro quo manner all of them offer their (frequently) free services in exchange for users' privacy. Activist practice, especially the type that aims to challenge the political status quo, requires maintaining a certain degree of clandestine engagement—at least during the planning stages, especially in the context of semi-authoritarian regimes. The political economy of commercial social media, based on complete transparency and monitoring of users' interactions, stands in stark contrast to such necessities.

Apart from continuous surveillance of their users in a commodifying manner, commercial social networking sites are unreliable for political activism due to the fact that these companies quite often face an unfortunate choice: either to be blocked by the government's censorship apparatus, or to agree to take down content, at least in the given country (York 2014).

Although in this article I focus on the case of the dispersion of Azerbaijani commercial social media based activism, interestingly enough Azerbaijan does not figure (at all) in neither Facebook's, nor Twitter's transparency reports, which disclose governmental requests for the removal of certain content. Turkey, on the other hand, is highly ranked in Facebook's report, and is an unrivaled leader in Twitter's (Facebook 2016; Twitter 2016).

This situation can be related to the crucial difference in tactics Azerbaijan and Turkey employ to silence online opposition—as it was already detailed, whereas Turkey simply blocks access to or censors the content of critical Internet media, Azerbaijan follows the approach of networked authoritarianism. Through the implementation of this technique from the early beginning, and by "simultaneously marginalizing the older opposition and forestalling the organization of younger activists", Azerbaijani government managed to effectively eliminate all alternative viewpoints, and to insulate itself from oppositional challengers (LaPorte 2015, 358).

Zeynep Tufekci argues that Turkish state officials, impressed by the Azerbaijani outcome, tried to apply networked authoritarianism in Turkey, and initiated a fear-mongering campaign against social media—depicting social networking sites as a "disruption of family, as a threat to unity, as an outside blade tearing at the fabric of society" (Tufekci 2014). Nevertheless, as social networks were already well embraced in Turkey, and were among the beloved tools of ordinary population, government had to suffice with the old habit of banning Internet sites.

4.2. The Unbearable Lightness of Hacktivism

The main principles of Anonymous' hacktivist operations, their workflows, and especially the tools the collective uses for these purposes are widely known. The main reason for this is that Anonymous itself promotes such openness in order to engage more people into the conduct of its DDoS acts. The main software tool, most commonly used by Anonymous while conducting Internet service disruptions, is a computer application known as the Low Orbit Ion Cannon (LOIC). This program was originally developed and distributed as open-source software, with the aim of server stress-testing (Sauter 2013, 993). It was initially intended to provide system administrators with a tool, suitable to test the performance of their servers under excessive HTTP requests, pinpointing critical performance issues. As the logic behind a simulated server stress-testing and a DDoS action is very similar, LOIC was quickly appropriated for the purposes of hacktivism.

DDoS attacks are computer assaults that aim to disable website servers from delivering proper services. They are based on the use of brute force, and thus procure their disruptive power from the sheer number of people participating in them: higher the number, faster and more devastating is the impact of the attack—but the number of users, participating in these attacks, is important not only for the magnitude of destruction.

For a long time, the use of LOIC in DDoS attacks was considered to be safe not because the tool anonymizes "your IP address […] but because the huge numbers of individuals participating would make it nearly impossible, or at least unduly inconvenient, for authorities to track down and arrest everyone" (Coleman 2014, 133).

So, in reality LOIC does nothing to conceal the identity of its user. Some other available DDoS tools have more advanced features, which allow their user to generate fake IP addresses, and assign them to the packets send by the program while establishing connection with the attacked server. This never was the case with any version of LOIC: all data packets sent with this application contain the real IP addresses of their senders. Internet Service Providers (ISPs) maintain the records of all IP addresses available within their networks and "can match those IP records to the real names and addresses of their subscribers" (Sauter 2014, 101–102).

This exactly was the case in Anonymous' #OpTurkey attacks, where only in matter of four days Turkish participants were identified, raided and arrested. Despite the above-mentioned facts about the unsafe nature of LOIC tool, a common knowledge among seasoned computer users interested in cyber security issues, many participants of DDoS attacks are not even aware of them. Ordinary actors of many DDoS campaigns who usually use the standard version of LOIC are not sophisticated computer users, and are frequently recruited through calls for action, placed on bulletin boards and Internet forums, like in the case of #OpTurkey.

Being only amateur enthusiasts, they frequently lack the most basic understanding of how cyberattack software really works (Coleman 2014, 134)—and whereas an experienced user might be aware of the fact "that running LOIC through a proxy or a spoofed IP address would provide some measure of protection from the security flaws in the tool", it is quite unlikely that someone who is new to "digital activism would be aware those tools existed or would understand how to operate them" (Sauter 2014, 102).

Anonymous is frequently labeled as a hacker collective, especially in mainstream media accounts of their activities—but, even if there is no dispute about Anonymous having highly skilled hackers among its members, in performing its attacks the collective quite often relies on "fairly simple vulnerabilities (such as SQLi)" (Rodriguez and Martinez 2012, 16). The practices of hacking are (very) different from the practices of hacktivism, especially the type pro-

fessed by Anonymous. Whereas hacking is an act of (mostly) individual tinkering with hardware and software—of "seeking quality and excellence in technological production" (Coleman 2016, 162); of refining a computer code "until it could be refined no more" (Hafner and Markoff 1991, 11)—hacktivism in its essence is a mediatized, program-based and software coordinated, form of concerted collective action.

In this sense DDoS attacks are not that different from flash mobs. Flash mobs are defined as an "instance in which the potential of virtuality becomes realized", when a group of people organized in the virtual realm, albeit momentarily, are able to affect the physical one (Solander 2005, 11). This is not to suggest that hacktivism's importance should be devalued. What I seek to point out here is that even a flash mob, which most of the time is simply seen as an apolitical, fun seeking happening, requires a long planning time—some by coming together, others through the instruction videos placed on YouTube, flash mobs participants train themselves, practice their moves and choreograph their actions. Such refined preparations do not take place before the hacktivist attacks, thus endangering the "recent additions to the Anonymous DDoS army, 'n00bs' or 'newfags' in Anonymous parlance" (Sauter 2014, 102), leaving behind too many digital traces, and making themselves easily identifiable.

In this sense, being a hacker and being a hacktivist mean occupying two different ontological positions. They are not necessarily exclusive of each other, and yet they are different, due to the divergent sets of practices they employ. Every aficionado of hacker culture occasionally fantasizes about embodying *The Matrix*'s Neo, a "talented hacker who becomes the new Prometheus, the one who must […] inspire a revolution that will free people from the very machines they have created" (Mosco 2004, 48). However, imagining of becoming Neo, while in reality just using LOIC at the comfort of one's home by "simply entering the target address and clicking the temptingly giant button marked 'IMMA CHARGIN MAH LAZER'" (Coleman 2014, 102), is an act which diminishes the real value of hacktivism, and makes rookie hacktivists look like ordinary script kiddies: wannabe hackers who use techniques and scripts developed by others to exploit computer networks or deface websites—i.e. unskilled individuals who "discover nothing on their own, but rather just download goodies from the Web" (Mitnick and Simon 2005, 144).

Hacktivism is an important practice in its own nature, but it is a form of act, practitioners of which need to understand the shortcomings of, and work on improving its tools and its praxis. Done otherwise, the current way of practicing hacktivism—with a tool that easily gives away the real identity of its user—will only continue to endanger the inexperienced participants of DDoS campaigns, and lead to their detentions, since the case of arrested Turkish hacktivists, detected through their IP addresses, actually was not a novelty.

In December 2010, Anonymous launched series of massive DDoS attacks in support of Julian Assange and WikiLeaks, claiming to exact vengeance against any party complicit in the smearing campaign against them—PayPal's blog and the PayPal website, as well as the "Swedish prosecutor's websites […] and the websites of Senator Joe Leiberman, Sarah Palin, MasterCard, Visa, EveryDNS […] and others" (Coleman 2014, 126).

Once again LOIC was the main tool, put to use for the implementation of this large-scale DDoS campaign. In the coming months of the attacks, dozens of individuals, who took place in them and used LOIC without taking any security precautions, were detained and charged under the US Computer Fraud and Abuse Act—and it was revealed later "that those arrests were based on a master list of IP addresses collected by PayPal as its servers were struck by a massive wave of DDoS actions on December 9 and 10" (Sauter 2014, 103).

5. Bringing Social Media Activism and Hacktivism Together

In an era of mediatization, where everyday communication practices are increasingly relying on, and are enacted through, media technologies, the way surveillance is conducted also transformed. The failure Anonymous experienced in Turkey, by using an outdated DDoS tool which makes its users easily identifiable, as well as the growing networked authoritarianism in Azerbaijan, are developments which are both enabled through widespread surveillance of Internet and mobile infrastructures.

Both in Turkey and Azerbaijan this pervasive surveillance was achieved, and is sustained, through a close collaboration of national intelligence and law enforcement agencies with local and international infotainment and telecommunications companies—and some private firms, specializing in the provision of various surveillance hardware, software and services.

For example, closely cooperating with Sweden's TeliaSonera, owner of leading Azerbaijani mobile network operator Azercell, the Azerbaijani state gained access to mobile telecommunications infrastructure, a privilege which was already in place back in 2009—clearly evident in the controversy over the questioning of all 43 Azerbaijanis who voted for the Armenian entry in the Eurovision song contest (BBC 2009). Legislation, forcing all of the country's mobile service providers to keep detailed logs of their users' telephone interactions and requiring "every mobile phone to be registered with the state communications authority (the Ministry of Communications and Information Technology)" (Callanan and Dries-Ziekenheiner 2012, 107) was passed and put into effect shortly after. In addition, the Azerbaijani state became one of the customers of the Italian cyber investigation company Hacking Team, obtaining their advisory services, as well as acquiring and widely using corporation's RCS software, a "sophisticated computer spyware marketed and sold exclusively to governments" (Marczak et al. 2014, 1).

Turkey—a long term NATO member and one of the few approved partners of the National Security Agency's (NSA) SIGINT division to host US equipment, to provide access to, and to collect data from submarine cables in exchange for access to gathered intelligence (Privacy International 2016, 46)—also undertook a similar approach, but on a grander scale.

For example, not only every imported phone needs to be registered with the authorities (or be blocked), but also mobile users are required to physically go to designated sale points to "provide proof of identification and sign a paper-based contract with their chosen mobile network operator" to tie the authenticated SIM card, including prepaid one, to their national identity number (GSMA 2013, 25). Additionally, a controversial law was put into effect, requiring all Internet companies in Turkey to store all Internet activity records (the traffic and browsing data) of their users for two years (ISPs were already required to do so for a long time)—and to provide this gathered data, including identifying information, to Telecommunications and Communication Authority (TİB) on request, without informing the user (APC and Hivos 2014, 249). Turkey as well is among the customers of Hacking Team—and in addition, purchased the Internet filtering program PackageShaper from Blue Coat Systems Inc., and acquired the advanced spyware FinFisher from UK-based Gamma International. These technologies are known to permit their customers to intercept passwords and emails as the "user of the device types them in and even remotely turn on a device's microphone to record" nearby conversations (Privacy International 2014, 7).

The increased monitoring of the activities, taking place in their respective cyberspaces, by the Azerbaijani and Turkish states is a development, paralleling global trends. As the sensational revelations of the NSA whistleblower Edward Snowden and WikiLeaks clearly showed, the claim about the extensive surveillance, conducted on a global scale by US and European intelligence agencies—in a close cooperation with a number of private companies—is true. Although for long time this claim was labeled as a conspiracy theory or simply ignored, the stash of documents, smuggled from the computer servers of US secret services, clearly indicates that we are indeed living in a type of society which was long ago dubbed as the surveillance society (Lyon 2001), or, as more recently, the surveillant society (Mathiesen 2013).

These types of societies rapidly emerge all around the world—in this era of radical socio-economic change, where the "privatization of both public space and public interest reaches a new level", and leaves states and governments with the perturbed choice of "either disappear or operate like a business" (Mosco 2004, 112). After all, the demographic categorizations of population, as done by the state bureaucracies; the threat analyses (and racial profiling practices) of intelligence agencies; and the packaging of users into clusters, in order to sell them as audience commodities to third party advertisers, as done by commercial social media platforms; are all activities that are operated in a certain concert with each other.

All of these acts are in a complete concordance, as all of them obtain their raw materials—the information about their users and their citizens—through extensive data- and infor-

mation-gathering. All of these activities are conducted with the same sets of electronic tools and with the same clusters of digital devices; with the same supercomputers and with the same data-processing methods; with the same purposes and through the same mindsets.

It should be of little surprise then that the same algorithmic computations, which Google and Facebook use to analyze their users' preferences and to provide them with targeted advertising, are being experimented upon by countries like China to develop individualized censorship mechanisms—to try to build "censorship engines powered by recommendation technology similar to that of Amazon and Netflix" (Morozov 2011, 100).

These experimentations clearly highlight the fact that the policies of global IT giants, the profiling techniques used to "improve the relevance of individually targeted advertisements", are compatible with authoritarian control systems, as they can easily be "used to refine individually targeted censorship and repression" (Ippolita 2015, 89). These systems can be fine-tuned to such a degree that only certain website addresses will be censored; or that certain Internet users only will be prevented from accessing them. Thus, mediatized surveillance, the conduct of which depends on the increase in the use of contemporary media technologies, enables more scrupulous, more individualized types of surveillance to be enacted, as surveillance shifts towards a new level of monitoring: *identity-based surveillance*.

This is a type of tracking which enables focusing, when necessary, specifically on the "elder, children, women, unhealthy, homosexual, homeless people, racially different and immigrant populations—in brief, all the 'others' of different social, cultural and economic contexts" (Mehrabov 2015a, 120).

It is obvious that the intertwining of surveillance, conducted for political purposes by state, with surveillance, conducted for economic purposes by private companies—as evident in the case of thousands of technology, finance and manufacturing companies (including makers of hardware and software, banks, Internet security providers, and satellite telecommunications firms) working closely with US national security agencies, and providing sensitive information to receive benefits, that included accessing classified intelligence and infiltrating adversaries' computers (Riley 2013)—forms a new sort of opponent.

This is an oppressor, which is much stronger and a more resilient one, which "not only is resistant to the old weapons but actually thrives on them" (Hardt and Negri 2000, 138). The emergence of this new opponent is in line with the emergence of a "negative dialectic of the enlightenment", where on a daily basis the "very liberal values of the enlightenment, such as the freedoms of thought, speech, press and assembly as well as the security of the people's persons, houses, papers and effects" (Fuchs 2014, 84) are constantly being undermined.

These changes require a careful evaluation of the strengths and the weaknesses of different forms of mediatized activism—of social media based activism and hacktivism—and finding mutual grounds between them, ways of bringing them together. This becomes especially urgent when taking into consideration that state intelligence agencies and private firms, especially the ones that thrive on surveillance of communication, often employ bright scientists, clever engineers and talented technicians. These entities do not shy away from even using services of their past antagonists—experienced cyber experts such as Kevin Mitnick, once a superstar of underground hacker scene, who now offers his skills as computer security consultant to world's largest companies and the FBI.

5.1. Strengths and Weaknesses of Hacktivism

There are a number of features that make the hacktivist group Anonymous truly unique. This collective is argued to simultaneously be a social movement and an anti-movement. The group is said to bear within itself individual fun and entertainment, as well as the nucleus of "collective political action based on a shared identification with some basic values ([…] civil liberties and freedom of the Internet)" (Fuchs 2013, 347).

These aspects, which frequently are told to be the forte of the group, are also its very own weaknesses. The described structure of Anonymous is reminiscent of *the union of egoists*, a term coined by Max Stirner to describe a "constantly shifting alliance which enables individuals to unite without loss of sovereignty"—a temporary hookup which "constitutes a purely

instrumental association whose good is solely the advantages that individuals derive from pursuit of their interests: there are no shared final ends, and association is not valued in itself" (Stirner 1995, xxix-xxx).

Although Anonymous is said not to be a purely leaderless, decentralized group, as it has its own core activists with "specific technical skills, media skills, and organisational skills who carry out the core of hacking activities" (Fuchs 2013, 349), it is questionable whether these cadres can be labeled as the "organic intellectuals" of hacktivist movement (Gramsci 1971).

The structural logic of Anonymous is a specific one: Anonymous' hacktivists are not familiar with each other and (mostly) have never met, and yet are able to act in coordination as one group (Fuchs 2013, 348). But, due to this specific logic, such online collectives are more prone to manipulation from the outsiders, especially law enforcement and intelligence agencies. It has been argued that the US hacker scene had been so densely infiltrated by security services that it is now filled with mutual mistrust (and paranoia) on the part of its members, since (approximately) one quarter of computer hackers secretly inform on each other to FBI (Pilkington 2011).

An interesting counter-example for such a loose organizational structure of Anonymous might be the Turkish hacker group RedHack, founded in 1997. RedHack describes itself as a Marxist-socialist collective and has a core team, which consists of only twelve members (Polat, Tokgöz Bakıroğlu and Demirhan Sayın 2013, 630).

RedHack possesses a very controversial position within Turkish society as their hacking activities range from attacks on bank systems to the "annulment of traffic tickets in Istanbul"; from disrupting "various governorship, district governorate and municipality websites" to making public the secret technical details of CCTV camera surveillance network, installed in Turkey (Uçkan 2013, 68).

The group gained wide popularity in Turkey after February 2012, when its members managed to hack into the National Police Directorate of Turkey. The members of RedHack were hailed as heroes, since they not only publicized secretive police documents, but also openly ridiculed an institution that was regarded in Turkey as the "key representative of security and state's coercion mechanism"—by exposing its laughable protection systems, such as system control passwords containing only consecutive numbers (Akın and Zıraman 2015, 16).

Thus, hacktivists (and hackers) can play a crucial role within the process of democratizing advanced communication technologies, and in attempts of making information available for a larger public. Based on their past exploits, as especially evident in the case of RedHack, they can even be characterized as capable fighters, who are "full of courage and tenacity in order to dare to attempt the most difficult" (Luxemburg 1918).

5.2. Activists' Own Social Media

A small portion of Anonymous' hacktivists seems to display tendencies, which parallel ones of RedHack. Dubbed as the cyber-socialist fraction, they consist of members who "stress the critique of class inequality between the rich and the poor, owners and non-owners, capitalists and workers" and crave for a non-corporate Internet that is "based on participatory democracy and socio-economic justice and equality" (Fuchs 2013, 369). So, ideologically solid collectives such as RedHack and the cyber-socialist fraction of Anonymous can be seen as prominent candidates for blending the differing practices of mediatized activism.

An attempt for such merging necessitates establishing non-commercial social media platforms, which can get various activist groups together. These sites need to implement socialist privacy politics and be operated within an economical structure, which is not guided by the aim of profit making—these alternative social media instead need to be "controlled and managed by prosumers, consumers, and producers" (Fuchs 2012, 148).

Within classic Marxist theory, re-appropriating the means of production forms the basis for the liberation of working class. But production for the sake of production is not a meaningful, sustainable process. When writing about the intertwined relation of production with consumption, Karl Marx was warning that "without production, no consumption; but also, without consumption, no production; since production would then be purposeless" (Marx 1973, 91). The

number of individuals, frustrated with commercial social media platforms, and aware that all these networks operate with an economic logic, based on perpetual monitoring and constant surveillance of their users, is rapidly growing. Especially after the disclosures of WikiLeaks and Edward Snowden, an increasing number of people started to notice the imminent danger (and threat) posed by various intelligence gathering entities—which blatantly thrive on acquisition of private user data, obtained (mainly) from the for-profit social networking sites.

diaspora*[8], and lately Minds[9], are social media platforms, praised for being developed as open-source alternatives to Facebook. diaspora* is a distributed, user-owned social network, run in a de-centralized manner (additionally providing Tor .onion service), and consisting of a number of personal web servers, which function as independent pods. Following the suicide of Ilya Zhitomirskiy, one of the co-founders and developers of the platform, in 2012 diaspora* was consigned to its users and turned into a community project, where users themselves are now responsible for developing and managing the network. diaspora*'s decentralized nature, where pods are administered by individual users, is seriously challenging the reliability of the platform for communicative purposes, as its protocol settings require that both the sending and receiving server are "online in order for a successful transaction to take place"—even in 2011, at the very peak of diaspora*'s popularity, only "20% of servers had over 90% uptime" (Bielenberg et al. 2012, 16).

On the other hand, Minds, initially supported by Anonymous, places the emphasis on the asymmetric encryption of user data; ciphers private messages, exchanged between the platform's users; and, powered by virtual currency Bitcoin, employs an economic model, where, through peer-to-peer advertising, users can exchange money for sharing content with others. The commercial structure deployed by Minds ensures that all of its users have a digital wallet and "earn points for every action, from voting on objects to sharing, commenting on a friend's post, or uploading their own pictures and videos"—where the network itself profits from multiple sources: from user payments to boost content; from running pre-roll video ads; and from "selling, on a subscription basis, the chance of creating one's own social network using the Minds.com framework and infrastructure" (Guerrini 2015). Thus, despite being celebrated by (especially) mainstream media as the platform, suitable for "those with a cause, who want to build something and share it openly with others who may also have a cause" (Collins 2015), essentially Minds is just another commercial service—with (slightly) better privacy settings.

5.3. Towards a New Model

Gustav Landauer, one of the leading theorists of German anarchist movement in the end of the 19th century, defined capitalist state as a "social relationship; a certain way of people relating to one another"—asserting that it can only be transformed by starting new forms of social relationships, by "people relating to one another differently" (Landauer 2010, 214).

The alternative, non-profit and non-commercial social media platforms can indeed turn out to be the facilitators of such renewed relationships. But envisioning such networks only as an alternative for Facebook, as in the cases of diaspora* and Minds, will be diminishing the role these platforms can play in blending various types of activist movements, in merging different dissent practices, in bringing the online forms of protest together with the offline ones. Roger Silverstone contended that,

> media, as indeed other technologies, enable the stretching of action beyond face-to-face, and consequently undermine the expectation of responsibility and reciprocity that action and communication in face-to-face settings conventionally require. Technologies disconnect as well as connect. The distance they create between interlocutors, between subject and subject, is a precondition, as many have argued, for the erosion of any sense of responsibility that individuals would be expected to have for the other (Silverstone 2007, 11).

[8] https://joindiaspora.com/
[9] https://www.minds.com/

I argue that formation of a new alternative non-commercial social media site can facilitate the revival of this sense of responsibility—by providing a platform where all different types of progressive activists can meet and discuss; work on strategies of mobilizing and recruiting new members; work out various ways of collaborating with each other and forming new alliances. This online space requires settings, which are different from those of for-profit social media—which systematically propagate the so-called culture of transparency and openness, only to commodify the generated user data.

The conceived non-profit social media platform needs to employ a central encrypted core, which will serve the function of a safe, surveillance-free communication space for the leaders of various movements to meet. This could be devised as a secure zone, where the emerging leaders of different movements (and their organic intellectuals) can gather and confidentially plan their actions.

Although the horizontality and the leaderlessness of recent square movements—Maidan, Syntagma, Tahrir and Taksim—have been highly praised, the lack of leaders proved to be a doomed choice for many of these protests. A revived debate about the importance of leaders in social movements ensued—due to the "blatant inefficiency of popular assemblies in making decisions and providing a direction for the movement" (Gerbaudo 2014).

Thus, the network's core needs to be visible to, and accessible by only the activist leadership cadres—the ones, who have been provided with the special electronic identification and the cryptographic authentication certificates to log in to the core. Steganographic techniques can be used to conceal this encrypted core from the plain sight—to confuse online snoopers, web crawlers and indexing bots; and to deceive advanced tracking spyware. Strong countermeasures and powerful security technology safeguards, such as intrusion detection systems and firewalls, need to be deployed to prevent cyberattacks and the attempts of unauthorized access.

Apart from the core, specifically designed for the needs of the leadership, a second level of this non-commercial alternative social media site can function as a regular social network. This public level can be used as the main medium through which various activist movements can disseminate their ideas and discuss their strategies with the rest of the cadres and the general audiences, sympathetic to social causes; and where, through the encrypted chat and messaging functionalities, members can also communicate among themselves.

This level can be used by social media based activists to call for their offline protests and to organize them more efficiently; and by hacktivist movements to engage people into participating in DDoS campaigns. Here hacktivists can teach their entrants how to use cyberattack tools, how to generate fake IP addresses and how to anonymize their identities.

It is through an alternative platform such as the envisioned one that hacktivists can, without endangering their participants, reach the critical mass necessary for the successful DDoS actions. As in any other social movement, robust public participation during hacktivist attacks is required for a variety of reasons—to give the conducted operation the moral gravitas and authority, and to convey a potent message through the strength in numbers (Coleman 2014, 138). Additionally, through the public level, alliances can be forged and collaborations can be started with other non-commercial alternative networks that "withdraw social media from corporate control and make state control of activist communication more difficult" (Fuchs 2014, 95); and the further facilitating of the copyleft culture can be undertaken (Mehrabov 2013).

This alternative social media platform needs to be non-profit, non-commercial, and ad-free—and at the same time financially independent. The fiscal sovereignty can be preserved with donations, collected through online crowdfunding and offline fundraiser campaigns; by introduction of membership fee, a common practice among political organizations to ensure economic sustainability of the movement; and with grants, received from progressive civil society organizations. State funding for such an initiative can be a feasible option, but this idea can only work within democratic contexts—where a "certain amount of liberties and citizen rights still exist, where civil disobedience has a recognized value, and state-sponsored repression rarely endangers the lives of citizens" (Ippolita 2015, 80). In a different socio-political context, the involvement of state funding could (even further) intensify state surveil-

lance, as well as increase possibilities for the platform's infiltration by informants and agent provocateurs from state intelligence agencies and security services.

6. Conclusion

We live in an era of mediatization, where daily practices are (increasingly) being managed with, and shaped by, online communication channels and digital media technologies. One of the intrinsic features of mediatization is that surveillance can be detected at its principal core (Jansson 2012; Christensen and Jansson 2015).

All Internet platforms, mobile apps, media devices and online networks are based on, and are enabled by, the rapid developments in digital electronics. As such, they are prone to the processes of quantification and datafication—verifying identity, recording utilization, monitoring consumption, logging activity, tracking time, and tagging access—i.e. gathering data from their users, as well as obtaining information about their interactions.

The financial value placed upon data, obtained from tracking of Internet activities, drives state law enforcement agencies and security services to establish close links with companies that thrive on data acquisition, since in capitalist society mediatization metaprocess depends on the economic dimension: commercialization is the "basic process providing the stimulus to all action" (Krotz 2007, 259).

The amalgamation of the practices of these actors consequently results in a radical transformation of the ways modern surveillance functions—and leads to mediatized surveillance, which is changing the understanding of what user data is, and where it can be procured from. Now a whole range of novel networked interactive technologies—from wearable computers to smartphones, from Internet-of-Things devices to smart home appliances—can be used in monitoring the users and collecting their data (Ackerman and Thielman 2016).

These fundamental changes in the functioning of contemporary surveillance mechanisms require a very careful evaluation of modern activist practices—which are as well increasingly being transformed by mediatization metaprocess, and are now (to a large extent) dependent on commercial media platforms and technologies. This dependence on online channels, over which activists in practice have no (or very) little control—together with the false evaluations of power relations, turned upside down by mediatized surveillance—resulted in the failures of mediatized activism in 2011, both in Azerbaijan and Turkey.

In this article I theorized on the formation of an alternative online space, which can blend two distinct types of mediatized activism—social media based activism and hacktivism—and bring them together. Building a platform, like the one conceived, requires engagement from different groups: seasoned representatives of various activist movements; application coders and web developers; IT engineers and computer programmers; technologically-savvy artists and interface designers; hacktivists and experienced hackers. Through the course of the last few decades, the hacker culture, and the symbols associated with it, turned into a "symptom of a broader class struggle over information" (Wark 2006, 321)—so, collaborating with hackers while building an alternative platform, which can (probably) challenge the political status quo (among others), is important not only for the purposes of ensuring online security.

The envisioned platform, with its zones for discursive interaction and educative communication; and online spaces, where activists and their audience, sympathetic to social causes, can meet and "choreograph collective action" (Gerbaudo 2012, 4), can help in reconnecting activist movements with the rest of the public—especially the (otherwise consenting) middle classes of any political regime. Attempting such attachment is even more valuable within the context of semi-authoritarian states, where a mere "complaining is enough to feel the consequences of state monitoring" (Pearce and Kendzior 2012, 286)—thus, alternative social media network, which is free from state surveillance and commercialization, can be (exclusively) rewarding in such context, as it can help dissatisfied and silenced citizens in revitalizing their online engagement. In concert with the activists of different social movements, ordinary people can come together; discuss their common future; develop communal strategies; plan joint operations; and finally reach out to the rest of the society and take their actions to the realm of the offline—to the mundane everyday life, where the social change really starts.

References

Ackerman, Spencer and Sam Thielman. 2016. US Intelligence Chief: We Might Use the Internet of Things to Spy on You. *The Guardian*, February 9. Accessed July 28, 2016. https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

Akın, Altuğ and Doğan Emrah Zıraman. 2015. Power Struggle in/around the Turkish Online Realm and Three Forms of Opposition: Redhack, Alternative IS Association and Personal Resistances against YouTube Ban. *GMJ: Mediterranean Edition* 10 (1): 13–21.

Amnesty International. 2014. *Behind Bars: Silencing Dissent in Azerbaijan*. London: Amnesty International.

Amnesty International. 2011a. *Azerbaijani Youth Activists Targeted after Using Facebook to Call for Protests*. London: Amnesty International.

Amnesty International. 2011b. *The Spring that Never Blossomed: Freedoms Suppressed in Azerbaijan*. London: Amnesty International.

APC and Hivos 2014. *Global Information Society Watch 2014: Communications Surveillance in the Digital Age*. Johannesburg and The Hague: Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos).

ARTICLE 19. 2012. *Running Scared: Azerbaijan's Silenced Voices*. London: ARTICLE 19.

Barry, Ellen. 2011. A Dissident Is Free From Jail, but His Punishment Is Not Over. *The New York Times,* June 24. Accessed May 20, 2016. http://www.nytimes.com/2011/06/25/world/europe/25azerbaijan.html

BBC. 2009. Azerbaijanis in Eurovision Probe. *BBC*, August 18. Accessed July 27, 2016. http://news.bbc.co.uk/2/hi/europe/8205907.stm

Bedford, Sofie. 2014. Political Mobilization in Azerbaijan—The January 2013 Protests and Beyond. *Demokratizatsiya: The Journal of Post-Soviet Democratization* 22 (1): 3–14.

Bielenberg, Ames, Lara Helm, Anthony Gentilucci, Dan Stefanescu and Honggang Zhang. 2012. The Growth of Diaspora—A Decentralized Online Social Network in the Wild. In *2012 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS 2012)*, edited by IEEE, 13–18. New York: IEEE.

Butler, Daren. 2011. Turkish Websites Attacked by Anonymous before Vote. *Reuters*, June 9. Accessed May 20, 2016. http://www.reuters.com/article/2011/06/09/us-turkey-election-internet-idUSTRE7583DV20110609

Callanan, Cormac and Hein Dries-Ziekenheiner. 2012. *Safety on the Line: Exposing the Myth of Mobile Communication Security*. Washington, DC: Freedom House/Broadcasting Board of Governors.

Carr, Jeffrey. 2012. *Inside Cyber Warfare*. 2nd ed. Sebastopol, CA: O'Reilly.

Champion, Marc. 2011. Turkey Arrests Alleged Hackers. *The Wall Street Journal*, June 14. Accessed May 20, 2016. http://online.wsj.com/news/articles/SB10001424052702303848104576383851077809420

Christensen, Miyase and André Jansson. 2015. Complicit Surveillance, Interveillance, and the Question of Cosmopolitanism: Toward a Phenomenological Understanding of Mediatization. *New Media & Society* 17 (9): 1473–1491.

Coleman, Gabriella. 2016. Hacker. In *Digital Keywords: A Vocabulary of Information Society and Culture*, edited by Benjamin Peters, 158–172. Princeton: Princeton University Press.

Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.

Collins, Katie. 2015. Anonymous Backs Encrypted Social Network 'Minds'. *Wired*, June 16. Accessed August 18, 2016. http://www.wired.co.uk/article/anonymous-backs-encrypted-social-network-minds

European Stability Initiative. 2011. *Generation Facebook in Baku: Adnan, Emin and the Future of Dissent in Azerbaijan*. Berlin-Istanbul: European Stability Initiative.

Facebook. 2016. Government Requests Report. Accessed September 11, 2016. https://govtrequests.facebook.com/

Fraser, Nancy. 1992. Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy. In *Habermas and the Public Sphere*, edited by Craig Calhoun, 109–142. Cambridge, Massachusetts: MIT Press.

Freedom House. 2012. *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*. New York: Freedom House.

Freedom House. 2011. *Freedom on the Net 2011: A Global Assessment of Internet and Digital Media*. New York: Freedom House.
Fuchs, Christian. 2014. Social Media and the Public Sphere. *tripleC: Communication, Capitalism & Critique* 12 (1): 57–101.
Fuchs, Christian. 2013. The Anonymous Movement in the Context of Liberalism and Socialism. *Interface: A Journal for and about Social Movements* 5 (2): 345–376.
Fuchs, Christian. 2012. The Political Economy of Privacy on Facebook. *Television & New Media* 13 (2): 139–159.
Gerbaudo, Paolo. 2014. Leaderless No More. *OpenDemocracy*, December 11. Accessed May 20, 2016. https://www.opendemocracy.net/can-europe-make-it/paolo-gerbaudo/leaderless-no-more
Gerbaudo, Paolo. 2012. *Tweets and the Streets: Social Media and Contemporary Activism*. London: Pluto Press.
Geybullayeva, Arzu. 2011. From Facebook to the Streets of Baku. *OBC Transeuropa*, March 12. Accessed August 11, 2016. http://www.balcanicaucaso.org/eng/Areas/Azerbaijan/From-Facebook-to-the-streets-of-Baku-93251
Gramsci, Antonio. 1971. *Selections from the Prison Notebooks*. New York: International Publishers.
GSMA. 2013. *The Mandatory Registration of Prepaid SIM Card Users*. London: GSMA.
Guerrini, Federico. 2015. Struggling With Facebook Organic Reach Decline? Try This New Open Source Social Networking App. *Forbes*, June 15. Accessed August 18, 2016. http://www.forbes.com/sites/federicoguerrini/2015/06/15/struggling-with-facebook-organic-reach-decline-try-this-new-open-source-social-networking-app/
Hafner, Katie and John Markoff. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.
Hardt, Michael and Antonio Negri. 2000. *Empire*. Cambridge, Massachusetts: Harvard University Press.
Harris, Sarah K. 2015. Networked Erasure: Visualizing Information Censorship in Turkey. *Convergence: The International Journal of Research into New Media Technologies* 21 (2): 257–278.
Human Rights Watch. 2012. *World Report 2012: Events of 2011*. New York: Seven Stories Press.
Hürriyet Daily News. 2011. Turkey Conducts Cyber Terror Drill. *Hürriyet Daily News*, January 27. Accessed July 27, 2016. http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkey-conducts-cyber-terror-drill-2011-01-27
Ippolita. 2015. *The Facebook Aquarium: The Resistible Rise of Anarcho-Capitalism*. Amsterdam: Institute of Network Cultures.
Jansson, André. 2012. Perceptions of Surveillance: Reflexivity and Trust in a Mediatized World (The Case of Sweden). *European Journal of Communication* 27 (4): 410–427.
Krotz, Friedrich. 2009. Mediatization: A Concept with Which to Grasp Media and Societal Change. In *Mediatization: Concept, Changes, Consequences*, edited by Knut Lundby, 21–40. New York: Peter Lang.
Krotz, Friedrich. 2007. The Meta-Process of 'Mediatization' as a Conceptual Frame. *Global Media and Communication* 3 (3): 256–260.
Landauer, Gustav. 2010. *Revolution and Other Writings: A Political Reader*. Oakland, California: PM Press.
LaPorte, Jody. 2015. Hidden in Plain Sight: Political Opposition and Hegemonic Authoritarianism in Azerbaijan. *Post-Soviet Affairs* 31 (4): 339–366.
Luxemburg, Rosa. 1918. The Socialisation of Society. *Marxists.org*. Accessed May 20, 2016. https://www.marxists.org/archive/luxemburg/1918/12/20.htm
Lyon, David. 2001. *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.
MacKinnon, Rebecca. 2011. China's "Networked Authoritarianism". *Journal of Democracy* 22 (2): 32–46.
Marczak, Bill, Claudio Guarnieri, Morgan Marquis-Boire and John Scott-Railton. 2014. Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab Research Brief #33*. Accessed July 21, 2016. https://citizenlab.org/wp-content/uploads/2015/03/Mapping-Hacking-Team's-_Untraceable_-Spyware.pdf
Marx, Karl. 1973. *Grundrisse: Introduction to the Critique of Political Economy*. New York: Random House.
Mathiesen, Thomas. 2013. *Towards a Surveillant Society: The Rise of Surveillance Systems in Europe*. Hampshire: Waterside Press.

Mattoni, Alice and Emiliano Treré. 2014. Media Practices, Mediation Processes, and Mediatization in the Study of Social Movements. *Communication Theory* 24 (3): 252–271.
Mehrabov, Ilkin. 2016. Azerbaijani Women, Online Mediatized Activism and Offline Mass Mobilization. *Social Sciences* 5 (4), 60. DOI: http://dx.doi.org/10.3390/socsci5040060
Mehrabov, Ilkin. 2015a. Exploring Terra Incognita: Mapping Surveillance Studies from the Perspective of Media and Communication Research. *Surveillance & Society* 13 (1): 117–126.
Mehrabov, Ilkin. 2015b. Gendered Surveillance and Media Usage in Post-Soviet Space: The Case of Azerbaijan. *Baltic Worlds* 8 (1–2): 44–48.
Mehrabov, Ilkin. 2013. Turkey and Copyleft Music Production: Reflections on Bandista. *IASPM@Journal: Journal of the International Association for the Study of Popular Music* 3 (1): 80–90.
Mitnick, Kevin D. and William L. Simon. 2005. *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders, and Deceivers*. Indianapolis, Indiana: Wiley Publishing.
Morozov, Evgeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs.
Mosco, Vincent. 2004. *The Digital Sublime: Myth, Power, and Cyberspace.* Cambridge, Massachusetts: MIT Press.
Pearce, Katy. 2014. Two Can Play at That Game: Social Media Opportunities in Azerbaijan for Government and Opposition. *Demokratizatsiya: The Journal of Post-Soviet Democratization* 22 (1): 39–66.
Pearce, Katy and Adnan Hajizada. 2014. No Laughing Matter. Humor as a Means of Dissent in the Digital Era: The Case of Authoritarian Azerbaijan. *Demokratizatsiya: The Journal of Post-Soviet Democratization* 22 (1): 67–85.
Pearce, Katy E. and Sarah Kendzior. 2012. Networked Authoritarianism and Social Media in Azerbaijan. *Journal of Communication* 62 (2): 283–298.
Pilkington, Ed. 2011. One in Four US Hackers 'Is an FBI Informer'. *The Guardian,* June 6. Accessed May 20, 2016. http://www.guardian.co.uk/technology/2011/jun/06/us-hackers-fbi-informer
Polat, Burak, Cemile Tokgöz Bakıroğlu and Mira Elif Demirhan Sayın. 2013. Hactivism in Turkey: The Case of Redhack. *Mediterranean Journal of Social Sciences* 4 (9): 628–636.
Privacy International. 2016. *The Global Surveillance Industry*. London: Privacy International.
Privacy International. 2014. The Right to Privacy in Turkey. *Universal Periodic Review Stakeholder Report #21*. Accessed April 17, 2016. https://www.privacyinternational.org/node/379
Reporters without Borders. 2012. *Internet Enemies Report 2012*. Paris: Reporters without Borders.
Reporters without Borders. 2011. *Internet Enemies*. Paris: Reporters without Borders.
Riley, Michael. 2013. U.S. Agencies Said to Swap Data With Thousands of Firms. *Bloomberg*, June 15. Accessed August 12, 2016. http://www.bloomberg.com/news/articles/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms
Rodriguez, Chris and Richard Martinez. 2012. *The Growing Hacking Threat to Websites: An Ongoing Commitment to Web Application Security*. Mountain View, California: Frost & Sullivan.
Sauter, Molly. 2014. *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.
Sauter, Molly. 2013. "LOIC Will Tear Us Apart": The Impact of Tool Design and Media Portrayals in the Success of Activist DDOS Attacks. *American Behavioral Scientist* 57 (7): 983–1007.
Silverstone, Roger. 2007. *Media and Morality: On the Rise of the Mediapolis.* Cambridge: Polity Press.
Solander, Carl. 2005. Placing Virtuality: Flash Mobs, Electronic Disturbance, and the War of the Worlds. *Thresholds* 29: 11–15.
Stirner, Max. 1995. *The Ego and Its Own*. Cambridge: Cambridge University Press.
Şardan, Tolga. 2011. Siber Saldırıda Dev Operasyon. *Milliyet*, June 11. Accessed May 20, 2016. http://www.milliyet.com.tr/siber-saldirida-dev-operasyon/gundem/gundemdetay/12.06.2011/1401414/default.htm
Tai, Zixue. 2015. Networked Resistance: Digital Populism, Online Activism, and Mass Dissent in China. *Popular Communication* 13 (2): 120–131.
Tremlett, Giles. 2011. Turkish Arrests Intensify Global War between Hacker Activists and Police. *The Guardian*, June 13. Accessed July 24, 2016. https://www.theguardian.com/technology/2011/jun/13/turkish-arrests-global-war-hackers-police
Tufekci, Zeynep. 2014. Everyone Is Getting Turkey's Twitter Block Wrong: Turkey Isn't Trying to Be North Korea, China or Iran; It's Trying to Be Azerbaijan. *Medium*, March 24. Accessed August 13, 2016. https://medium.com/message/everyone-is-getting-turkeys-twitter-block-wrong-cb596ce5f27

Tunç, Aslı. 2013. Freedom of Expression Debates in Turkey: Acute Problems and New Hopes. *International Journal of Media & Cultural Politics* 9 (2): 153–163.
Twitter. 2016. Twitter Transparency Report. Accessed September 10, 2016. https://transparency.twitter.com/en.html
Uçkan, Özgür. 2013. Dijital Aktivizmin Sınır Boyunda Hacktivizm: Anonymous ve RedHack Örnekleri... In *Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Biçimi*, edited by Ali Rıza Keleş and Yetkin Sal, 53–79. Istanbul: Alternatif Bilişim Derneği.
Uldam, Julie. 2016. Corporate Management of Visibility and the Fantasy of the Post-Political: Social Media and Surveillance. *New Media & Society* 18 (2): 201–219
Wark, McKenzie. 2006. Hackers. *Theory, Culture & Society* 23 (2–3): 320–322.
York, Jillian C. 2014. Social Media Has Been Privatised. Why Do We Treat It as a Public Space? *New Statesman*, June 11. Accessed May 20, 2016. http://www.newstatesman.com/internet/2014/06/social-media-has-been-privatised-why-do-we-treat-it-public-space

About the Author

Ilkin Mehrabov
Ilkin Mehrabov is a PhD candidate in Geography, Media and Communication Studies at Karlstad University, Sweden. Of Azerbaijani origin, he conducted his previous studies in Turkey, obtaining degrees in Electrical-Electronics Engineering and Media and Cultural Studies, both from Middle East Technical University, Ankara. His doctoral dissertation focuses on changes in activist practice in relation to mediatization metaprocess, and pervasive public/private surveillance. His research interests and publications focus on alternative and activist media; citizen journalism; and social impacts of ICTs.