New Media Politics

New Media Politics:

Rethinking Activism and National Security in Cyberspace

Edited by

Banu Baybars-Hawks

Cambridge
Scholars
Publishing

New Media Politics:
Rethinking Activism and National Security in Cyberspace

Edited by Banu Baybars-Hawks

This book first published 2015

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-4438-7710-7
ISBN (13): 978-1-4438-7710-7

This book is dedicated to the memory of Dr. Dwight L. Teeter, Jr., a journalism historian and legal scholar. Dr. Teeter passed away on February 27, 2015. His academic career spanned fifty years and included teaching at the University of Texas at Austin, the University of Kentucky, and the University of Wisconsin at Madison. His last home institution was the University of Tennessee in Knoxville, where he served as dean of the College of Communications from 1991 to 2002 and continued to teach as a professor until he retired at the end of 2014.

Dr. Teeter had a major impact on the lives of so many of his students and colleagues. With the announcement of his death, countless messages of mourning were shared at an interpersonal level and via social media. Some of the words or phrases used to describe Dr. Teeter were "witty," "genuine," "honest," "incredibly smart," and "class act." Many expressed how Dr. Teeter went beyond being an educator and was also a friend who often extended a helping hand and provided words of encouragement. Dr. Teeter genuinely cared about the well-being of others, and it was a great joy for him to see his students and mentees find success in life.

Dr. Teeter was passionate about the issues of press freedom and government transparency. In the 13th edition of his textbook *Law of Mass Communications*, Dr. Teeter expressed deep concern about the recent expansions of government secrecy and intrusions into privacy by the government, law enforcement agencies, and private businesses. This was a topic that he was looking forward to researching upon retirement. It is unfortunate that we will never have the opportunity to read the scholarly work that this brilliant scholar would have produced. Perhaps we may comfort ourselves with the knowledge that the many individuals inspired by Dr. Teeter's writings will in some way continue his work by asking difficult but important questions pertaining to the free flow of information and press freedom. Research that sought to reveal social injustices and protect vital social and political freedoms always brought a smile to Dr. Teeter's face. That smile will be profoundly missed, but fondly remembered.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

ACKNOWLEDGEMENTS

This edited volume is based on selected papers presented at a conference titled "New Media Politics: Conflict, Activism, and Security" (held at Kadir Has University in Istanbul in April 2014). I appreciate all the support I received from Kadir Has University, as well as my colleagues at the Faculty of Communications.

I would also like to thank all of the participants of the conference, as their presentations and discussions played a crucial role in shaping the structure of this edited volume.

Very special thanks to all of the contributors for the quality of the chapters and for their timely and kind responses to our every request, as well as their willingness to share their ideas with us while I was working on the volume. I would like to extend my gratitude to each, in order of appearance: Sarphan Uzunoğlu, Eser Selen, Yenal Göksun, Cristina Ivan, Eloisa Nos Aldas, Pantelis Vatikiotis, Hussni Nasr, Aşkın İnci Sökmen, Abdelrahman Rashdan, Sevda Ünal, Bilge Narin, Bahar Ayaz, Catherine A. Luther, Çağrı Yalkın, Suncem Koçer, and İrem İnceoğlu.

I greatly appreciate the assistance I received from Mark D. Wyers with proofreading the chapters.

And of course, I would like to thank Michael Dean Hawks, Derin Kyle Hawks and the other members of my family for always being there for me.

PART I.

CHAPTER ONE

INTRODUCTION— OCCUPYING CYBERSPACE: CYBERACTIVISM, CYBERTERRORISM AND CYBERSECURITY

BANU BAYBARS-HAWKS

A lot has changed in the world since the 9/11 terrorist attacks. The US, which has been held up as a leading advocate of fundamental freedoms, was attacked in the heart. This act of terrorism targeting the US raised many concerns and questions and created difficult ethical and professional challenges for democracies. The main concern was how to achieve a balance between state control and basic rights and freedoms, and whether such a balance is necessary. These issues are still discussed today at a time when societies are facing new threats and attacks in light of developments in technology, which has offered new alternatives for terrorist activities. As Yonah Alexander has noted:

> This threat has become much more decentralized as it now emanates not only from established organizations, but also from freelance individuals with the motives, means, and opportunity to visit harm upon civil society. As a result of these developments, contemporary terrorism presents a multitude of threats to safety, welfare, and civil rights of ordinary people; the stability of state systems; the health of national and international economic systems; and the expansion of democracies. (2011, x)

The attacks of 9/11 and the subsequent "war on terror" have been called the first war of the Internet age (Glass 2002). Terrorism today is at the intersection of radicalism and technology. In the past, enemies could be defined or confined geographically but now there are no clear geographical boundaries separating "us" from the enemy because they are able to take advantage of technology: "Non-state actors with their

asymmetrical force structures have overstepped the state boundaries and became global with the advent of information technologies and globalization" (Aydın, *Hurriyet Daily News*, January 15, 2015). With this new face, terrorism is more dangerous than ever because its origins may not be known and it may not be bound up with any given nation-state. Today's terrorists do not need planes, bombs and other such weapons to carry out attacks. They can infect important computer systems with viruses and paralyze the military, political and economic resources of a country, even a continent.

Cyberspace is an attractive venue for people hoping to carry out acts of terror because it is cheaper and more anonymous than traditional methods of terrorism. The variety of targets is also quite large, as is their number, and cyberterrorists can operate remotely: "Cyberterrorism requires less physical training, psychological investment, risk of mortality, and travel than conventional forms of terrorism, making it easier for terrorist organizations to recruit and retail followers" (Wiemann 2004, 5). Since cyberterrorism has a direct influence on a larger number of people than conventional terrorism, it generates more publicity and receives more media attention, which is precisely what terrorists seek.

Cyberspace is a key aspect of modern life, but the growing dependence of society on information technologies has created new vulnerabilities to terrorist attacks: "The more technologically developed a country is, the more vulnerable it becomes to cyberattacks against its infrastructure" (Wiemann 2004, 2). Cyberterrorism has been acknowledged by most governments as a serious national security concern. Jonathan Matusitz (2008) describes seven types of cyberterrorist activities: attacking infrastructure, commandeering nuclear power plants or hazardous waste facilities, using computers to control dam flows, hacking into power grids, using technology to commit sabotage, initiating protests that involve hacking government computers, and illegally compromising information accessed through computers.

One of the most important cyberterrorist attacks was the Stuxnet computer worm incident, which occurred in July of 2010. During the attack, Iranian computers were hacked with the aim of destroying plutonium enrichment plants, thus hampering the country's alleged efforts to develop a nuclear bomb. It was widely rumored that the attacks were engineered through a joint effort between the United States and Israel. Allegedly, Iran responded by launching a cyberattack on US financial institutions. In 2007, the Eastern European nation of Estonia was hit with a massive DoS attack that affected government and corporate websites. Estonia blamed the Russian government, which denied responsibility.

The products of popular culture have helped expand on fears of cyberterrorism. In June of 2003, the *Washington Post* published this front-page headline: "Cyber-Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say." In a movie titled *War Games* dating from 1983, a young hacker breaks into a US military supercomputer and sets in motion a chain of events that have the potential to start World War III. The theme of *GoldenEye*, a James Bond film, was also cyberterrorism. *Swordfish, Die Hard 4.0* and the TV series *24* are other examples. Novels about cyberterrorism include Tom Clancy's *Net Force* series, Winn Schwartau's *Pearl Harbor.com*, and James Dashner's *The Eye of Minds* and *The Rule of Thoughts*. Mass media is also likely to label hacking activities as acts of cyberterrorism. Therefore, it is important to separate "hacking" from "cyberterrorism," even though their borders are difficult to define.

Hacking has been described as covert activities conducted online that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software. While the aim of cyberterrorists is to kill or spread terror, hackers only seek to wreak havoc. However, the distinction between hacking and cyberterrorism sometimes blurs, such as when terrorist groups are able to recruit or hire hackers. Hackers can be turned into cyberterrorists, and this transition can be motivated by money or prestige. As young and educated people are brought into the fold of terrorist groups, this new generation will have the means to execute acts of cyberterrorism (Baybars-Hawks and Akser 2012).

As cyberspace is increasingly used for a variety of purposes by terrorists and hackers, different terms have arisen such as "hacktivisim." Hacktivism can be defined as "the nonviolent use of illegal or legally ambiguous digital tools in the pursuit of political ends." Hacktivist activities span many political ideals and issues. *Freenet* is a prime example of translating political thought (that anyone should be able to speak) into code. Hacktivism is an offshoot of the Cult of the Dead Cow, and its core belief is that access to information is a basic human right (Karatzogianni 2006).

Hacktivism is a controversial term, and can often be misconstrued as cyberterrorism, just as hacking. What separates hacktivism from cyberterrorism is a distinctly political or social cause behind the "haction." Some argue that it was coined to describe how electronic direct action might drive social change by combining programming skills with critical thinking. Others use it more or less synonymously with malicious, destructive acts that undermine the security of the Internet as a technical, economic and political platform.

Essentially, the controversy reflects two divergent philosophical strands within the hacktivist movement. One side argues that malicious cyber-attacks are an acceptable form of direct action (black hat hackers). The other side claims that all protests should be peaceful, refraining from destruction (white hat hackers) (PCtools.com, accessed October 12, 2014).

A major form of hacking called "denial of service" (DoS) attacks paralyze websites, financial networks and computer systems by transferring data to them from outside computers. A fifteen-year-old Canadian boy carried out the first documented DoS attack in 2000 against several e-commerce sites including eBay and Amazon, shutting some down and disrupting others at an estimated cost of $1.7 billion dollars.

Computer hackers have also targeted government and private web networks. For example, in 2006 the Pentagon reported six million attempts to break into its networks. This number has increased yearly, including a successful attempt supposedly originating in China to hack into the $300 billion dollar Joint Strike Fighter project and copy data about its design and electronics systems. According to computer experts, computer criminals in China and Russia have infiltrated the US electrical grid and installed software capable of damaging the system. In 2011 alone, the US Computer Emergency Readiness Team (US-CERT) responded to more than 106,000 cyber security threats and released more than 5,000 viable cybersecurity alerts to public and private sector partners (Burghardt 2013).

Private sector organizations and companies are often targeted by cybercriminals for both financial gain and political reasons. In November of 2014, Sony Pictures Entertainment suffered a massive data breach that froze its computer systems. In the days following the initial attack, the hackers who claimed responsibility for the breach posted data to an anonymous Internet posting board. The information leaked to the public included salary information, internal passwords, employee social security numbers, executive presentation slides, and a number of unreleased films (Savov 2014). In early 2015, a major leak occurred when information belonging to the account holders of HSBC Bank's Swiss branch was put online.

Hackers target ordinary citizens as well. On a regular basis news stories report about hackers raiding computer networks for social security numbers, banking and credit card information, and other information used for identity theft. In 2005, hackers breached the University of California's computer system and stole the social security numbers of 97,000 students, and the same happened again in 2009 (Dearen, August 5, 2009).

Social movements have increasingly been using advanced forms of communication technology as a means of mobilizing. These new forms of

technology are redefining political struggles by providing the resources and environment necessary for activist movements. It has been argued that the Internet is potentially "more persuasive and effective in diffusing social ideas and actions within a global community of interest than any other communication technology in history" (Castells 2001). Also, "Information on the Internet, not necessarily available in the mainstream press, and coming from alternative sources that otherwise may not be heard, enhances the resources available to actors in social and political struggles" (Meikle 2002; Pickerill 2003, in Carty & Onyett, 238). This has led to rapid, creative and universal action among activists. Although these new technologies make it easier to access information and resources to bring about social change, their role in helping movements grow has been questioned (Carty & Onyett 2006, 240). Advances in technology have also given rise to new social movements (NSMs): "NSMs are based on identity-issues and operate at the grassroots level. These are differentiated from previous, or 'old', movements that focused exclusively on class-based issues at the structural level" (Carty and Onyett 2006, 231).

Redefinitions of the concept of activism are indicative of the fact that activism has grown around issues selected by a group of individuals (Illia 2003, 326). These players include traditional pressure groups that go online, as well as spontaneous aggregation and individuals (327). Activist movements do not necessarily end up in actual protests, but cyberspace often serves as the initial platform for protest activities, as happened during the Arab Spring.

Cyberactivism, in other words, political activism on the Internet, often includes online activist strategies "from online awareness campaigns to Internet-transmitted laser-projected messaging" (McCaughey & Ayers 2003, 2). Cyberactivism has thus brought about new challenges regarding political organizing and social change: "For example, hacktivists conduct online sit-ins and deface Webpages as a form of protest" (McCaughey & Ayers, 5). Whether this action can be framed as a new form of political direct action or just a national security breach is an important question.

According to Sandor Vegh (in McCaughey & Ayers, 71), cyberactivist tactics can be categorized in three ways: awareness/advocacy, organization/mobilization, and action/reaction. An undeniable fact is that the Internet is increasingly being used in acts of resistance. Since cyberspace has become a platform for activist movements, governments and corporations have taken steps to ensure that they are prepared to deal with these threats: "As in the case of traditional resistance movements, by framing online activism as criminal activity or a national security threat, they reinforce their hegemonic grip on dissent" (Ibid. 93). Several chapters

in this book elaborate on the struggle between hegemonic structures and activist movements from different perspectives.

The ubiquitous nature of communication technologies has resulted in a variety of discussions regarding the regulation of cyberspace. One side argues that cyberspace should be a free democratic space, while the other focuses on cyberspace as a platform for crime, espionage, fraud, and even war and hence argues that it should be regulated (Kremer 2014, 220).

During the early years of Internet in the mid-1990s, many users believed and argued that the world of cyberspace should be free from all governmental regulation. "A Declaration of the Independence of Cyberspace," which was authored by John Perry Barlow, suggested that national governments should not play a role in governing cyberspace. He argued that the community existing in cyberspace would create its own rules and manage conflicts outside the jurisdiction of any particular country. Particularly important was the protection of free expression and exchange among the "bodiless" personalities of cyberspace: "The Internet can be used as place of freedom and of political activism, and can enable new forms of political participation and organization of democracy" (Kremer, 226). Organizations such as the Electronic Frontier Foundation (EFF), of which Barlow was a cofounder, were established with the aim of protecting cyberspace as a location for the free sharing of knowledge, ideas, culture and community. Such organizations pursue this goal through a variety of activities, including opposition to legislation seen to be in conflict with the free use of technology, launching court cases to preserve people's rights, and initiating publicity campaigns to inform and engage the public on issues of cyberspace and technology (Bussell 2007).

The main argument used to justify regulating cyberspace is the protection of national security. The fear that cyberspace can be used by extremists, terrorists and organized crime affiliates has driven technologically vulnerable societies to enact laws limiting access to cyberspace. Since state governments believe that threats to the security of their citizens and the stability of their regimes may arise from within cyberspace, they take measures to control both access and content. With this aim, they have developed new standards of safety as well as new forms of surveillance (Kremer 226). A few of the chapters in this book discuss these new forms of security challenges regarding cyberspace in terms of control and surveillance strategies that are being used in different countries. These include both state regulations and international agreements concerning the character of cyberspace. For example, the Chinese government, as with the Turkish government, maintains controls on who is able to access the Internet and what content is available. The US

government has placed restrictions on certain online activities, such as the sharing of digital data, through the Digital Millennium Copyright Act and other legislation, and it has also developed a strategy to ensure the security of cyberspace in order to prevent and respond to attacks on Internet infrastructure (Bussell 191). Shortly after taking office in 2009, President Barack Obama ordered a review of government efforts to defend US information and communications systems. According to Cyberspace Policy Review, the goal was to come up with an organized and unified response to future cyberthreats, strengthen public and private partnerships, find technological solutions to enhance US security and prosperity, and invest in cutting edge research and development. They also called for a campaign to promote cybersecurity awareness and digital literacy from boardrooms to classrooms and develop a twenty-first century digital workforce. In 2009, the Department of Homeland Security (DHS) launched the National Cyber Security and Communications Integration Center, a twenty-four-hour watch and warning center; it is also the country's principal hub for organizing cyber-response efforts and maintaining a comprehensive national outlook. In 2010, the DHS and the Department of Defense signed an agreement by the terms of which they will jointly counter threats to critical military and civilian computer systems and networks. The agreement embedded Department of Defense cyber analysts within the DHS and DHS personnel within the Department of Defense's National Security Agency (Bussell 2007).

Just as states have attempted to regulate cyberspace, international regulations regarding the control of cyberspace exist as well. One of the first international treaties on cybercrimes is the Council of Europe Convention on Cybercrime (Council of Europe Convention on Cybercrime, Budapest, 23 November 2001, ETS no.185). The Convention lists the crimes that are committed in cyberspace, including "computer-related fraud, forgery, system interference, computer misuse, child pornography and copyright infringements, [and] it attempts to bind states to include specific countermeasures within their legal systems," while at the same time it obliges states to "ensure the legal and factual possibilities for searching computers, real-time collection and also intercepting data" (Kremer, 234-35). Kremer points out that there are dangers in the criminalization of malicious acts in cyberspace since it could create opportunities for security agencies to expand their surveillance capabilities (235).

The chapters in this volume explore many of the questions surrounding the new challenges that have arisen as a result of the emergence of cyberspace, including cyber activism, cyberterrorism, and cyber security.

They provide case studies across an array of geographies as they debate questions regarding conceptual issues in cyberspace, the relationship between politics and cyberterrorism and cyber activism, state and international regulations concerning cyberspace, resistance movements in cyberspace, and media frameworks concerning terrorism, civil liberties, and government restrictions. By bringing this collection together, we hope to provide a venue for discussions of the diverse issues around the theme of new media politics from international and interdisciplinary perspectives. This volume is divided into two parts. The first part of the volume focuses on how cyberspace has been involved in activism, acts of resistance and protests. The second part of the volume investigates issues related to how online media is used in terrorism and how governments have sometimes perceived cyberspace as a threat, leading at times to regulations which threaten to curtail liberties in the name of protecting the "security" of the state against enemies that may be seen as "internal" or "external."

Part I

In Chapter 2 Sarphan Uzunoğlu focuses on the use of cyberspace by political activists and proposes that the secure and anonymous use of new media will be needed to replace the existing practice of surveillance in many democracies. In his analysis, he suggests that anonymity is a new means of organizing direct democracy in communities of various sizes, meaning that anonymity and semi-anonymity can provide citizens with secure access to political decision-making processes. In this way, the use of anonymity and semi-anonymity through hegemony may create a new and more democratic environment for both resistance and contemporary daily politics.

Eser Selen in Chapter 3 discusses the politics of resistance and reaches conclusions that in many ways support Uzunoğlu's arguments about the increasing usage and importance of new media tools in activist movements. Her case study is *The Electronic Intifada*, which is an online resource for media analysis, criticism, and activism focusing on Palestine, its people, politics, culture and place in the world, and which has played a significant role in the Israeli-Palestinian conflict and its transformation. Selen concludes by noting the effectiveness of *EI* in building a counter-hegemonic community: "...the real challenge in the kind of resistance that *EI* poses for the occupation is to transform the conflict through the global solidarity they generate while sustaining the resistance in order to achieve more concrete political results."

Similarly, Yenal Göksun in Chapter 4 investigates online political activism and how the Internet is being used as a tool for advocacy. He takes as his case study Syrian bloggers. Highlighting the Syrian government's strict control of cyberspace since the beginning of the uprising in the country, Göksun argues that blogging has given Syrian bloggers a non-violent space for expressing their opinions as the violence in society rages around them. The conflict in Syria motivated bloggers to focus on political issues and start discussions on topics which were previously seen as taboo. He concludes that Syrian blogs have shaped a new public sphere and helped create a civil society which will be necessary in the future.

In Chapter 5, Cristina Ivan focuses on the concept of hyper-reality and its implications in the area of activism. She argues that the complexities of the virtual online environment overlap "reality as we know it" and within this context she sees hyper-reality as one of the major catalysts and effects of globalization. Ivan also notes that active citizenship will not be possible in the absence of technology and hyper-reality. She concludes by arguing that real and simulated interactions between individuals, real world activism and virtual statements blend in a continuum, offering up a taste of future social patterns and behaviors as we witness the emergence of a new master-narrative of active citizenship in the search for meaningful causes.

Eloisa Nos Aldas in Chapter 6 explores new media activism by applying narrative power analysis and story-based strategies for social change. She reviews the cultural consequences of communicative innovations and the successes of engagement with the 15M movement in 2011 in Spain (the #SpanishRevolution) as well as around the world in digital networks. Aldas points out the potential and power of viral storytelling and cultural memes as a recent trend of social movements together with the options of information and participation made possible by transmedia as key elements in scenarios of social change. She argues that they have broken the spirals of silence described by Noelle Neumann (1974) and started a new era for social action and communication.

In Chapter 7, Pantelis Vatikiotis examines the dynamics of new mediated protest cycles and questions their dimensions in terms of: a) the "networked" structure of movements, b) their "(trans)national" echoes, and c) their "radical" perspective. This chapter emphasizes the need for an integrated approach to contemporary mediated forms of contention through the prism (concepts and tools) of media studies and social movement studies research. Vatikiotis points out the challenges that have been addressed by analyses of the interplay between protest movements

and media as a whole at the state and transnational levels in relation to constructions of the politics of conflict.

Hussni Nasr in Chapter 8 elaborates on the Internet's impacts on social movements. He specifically analyzes the role played by Facebook in the revolution in Egypt in 2011. By using content analysis, Nasr examines how Facebook posts and comments were framed to mobilize and advance an online revolution that activated an offline movement in Egypt. In conclusion, the author emphasizes the role of social media including the use of Facebook for posting citizen journalism accounts and the importance of interactivity among users via Facebook features such as the ability to "like" a comment or respond to another's comment. Nasr argues that these features contributed to the transition of the Egyptian movement from the online virtual realm to the offline real world.

Part II

In Chapter 9, Aşkın İnci Sökmen discusses the importance of globalization and the impacts of the information revolution on society, as well as their roles in changing our definitions of crime and conflict. She argues that netwar may well be the dominant mode of societal conflict in the new era, and points out that the distinguishing element of netwar is the network, not technology. Because networks motivate officials to build their own networks as well as hybrids of hierarchies and networks to deal with networked organizations, doctrines, and the strategies of their information-age adversaries, Netwars and counter-netwars have become pressing issues.

Abdelrahman Rashdan in Chapter 10 focuses on the problem that rapid developments in information technology have created for the Intelligence Community (IC). He observes that the main issue is not so much about using sophisticated technology effectively to keep a close eye on the open source information boost, but rather it is an "educational problem." Rashdan lists four main kinds of challenges that have been posed by social media as regards Open Source Intelligence (OSINT): knowledge management, the nature of data in terms of language and cultural context, access to data, and IC's "educational problem." He then offers strategies that could be used to solve those issues.

In Chapter 11 Sevda Ünal discusses the securitization of cyberspace. She claims that states have employed an argument of "risk" to justify practices of control and surveillance in cyberspace. She further observes that securitization in the name of preventing "risks" brings along problematic issues such as privacy, regulation, surveillance, censorship,

and Internet regulation while also creating tension in the international system. Her study concludes with a discussion of the state laws and regulations which have been developed in the name of ensuring security.

In Chapter 12, Bilge Narin and Bahar Ayaz offer conclusions regarding their content analysis of readers' comments for news related to an ISIS attack that was carried out in Turkey. The main aim of their research is to analyze user-generated content in online Turkish news about terrorism. Narin and Ayaz's study reveals that the narrative discourses used by readers of online news differ from reviews of traditional news about terrorism. Readers of online news both criticize and support terrorists' motives as well as the government's policies of security. Their comments conclude with the various new ways that terrorist acts can be linked to other events.

Catherine A. Luther in Chapter 13 discusses the types of surveillance activities that have been adopted in the name of national security in various democratic nations, including the United States. She then goes on to present a historical overview of US intelligence-gathering operations. Her chapter concludes with a discussion of the increase in new media usage by terrorist groups and its implications with regard to the future of state surveillance, and in turn, democratic governance.

In Chapter 14, Çağrı Yalkın shifts the focus to surveillance practices that have been used by the Turkish government as regards cyberspace. According to Yalkın, social media constitutes a politically charged space and this contested space thus provokes authoritarian governments to intervene in or censor the use of such platforms, which, in turn, triggers (politically charged) reactions and resistance. Within this context, she conceptualizes social media and the use and censoring of Twitter in Turkey as a public sphere in which agonistic pluralism is enacted, and she concludes that the way in which this destabilization pluralizes the public sphere in the case of Turkey is agonistic, as demonstrated by the two Twitter cases investigated in her study.

In Chapter 15, Suncem Koçer similarly dwells on the reactions of governments when social media is seen as posing a threat to the legitimacy of their existence. In response to the question of how political powers seek to retain hegemonic constructions of social and political life that are breached by the widespread use of social media, she argues that in order to contain dissent and the free-flow of information via social media, governments tend to produce discourses that criminalize the medium of popular mobilization. Additionally, she provides a semantic analysis of the president of Turkey's rhetoric on social media and notes the particular mechanisms of criminalization he uses.

İrem İnceoğlu in Chapter 16 elaborates on the arguments that have been used to discuss re-constructions of the Internet in accordance with its usage for various purposes. Within this context, she examines how the issues of security, individual rights and freedoms have been constructed as attempts to control the Internet and its users. İnceoğlu's analysis covers the case of Turkey from the year 2011 onward and discusses Internet censorship and surveillance, as well as the counter-culture that has arisen in response.

In Chapter 17 Banu Baybars-Hawks focuses on the interactions occurring between new media, government and society in Turkey as a result of the increasing use of social media by young users. She discusses the latest regulations drafted by the government regarding new media and points out that the restrictions on new media in Turkey amount to censorship. Baybars-Hawks further claims that limitations introduced by laws on new media should be proportional and in line with the requirements of democracy.

Works Cited

Alexander, Y. 2011. Foreword. In *If It was not for Terrorism- Crisis, Compromise, and Elite Discourse in the Age of "War on Terror,* eds. Banu Baybars Hawks & Lemi Baruh, ix-x. NE: Cambridge Scholars Publishing.

Akser, M and Baybars-Hawks, B. 2012. Media and Democracy in Turkey: Toward a Model of Neoliberal Media Autocracy. *Middle East Journal of Culture and Communication* 5: 302-321.

Aydın, M. 15 January 2015. The Challenge of Non-state Extremism. *Hurriyet Daily News.*

Burghardt, T. 2013. *The dark road from the clipper chip to Prism reveals 'Crypto Wars' never ended*. http://www.uncommonthought.com/mtblog/archives/2013/11/18/the-dark-road-f.php

Bussell, J. 2007. Cyberspace. In *Encyclopedia of Governance,* ed. Mark Bevir, 190-192. Thousand Oaks, CA: Sage Publications.

Carty, V. and Onyett, J. 2006. Protest, cyberactivism and new social movements: The reemergence of the peace movement post-9/11. *Social Movement Studies* 5(3): 229-249.

Castells, M. 2001. *Internet Galaxy: Reflections on the Internet*. Oxford: Oxford University Press.

Council of Europe Convention on Cybercrime, Budapest, 23 November 2001.

Dearen, J. 2009. Hackers breach US Berkeley computers. http://www.nbcnews.com/id/30645920/ns/technology_and_science-security/t/hackers-breach-uc-berkeley-computers/ Accessed February 23, 2015.

Glass, A.J. 2001. *The war on terrorism goes online: Media and government response to first post-Internet crisis*. Cambridge, MA: Harvard University, the Joan Shorenstein Center on the Press, Politics and Public Policy.

Illia, L. 2003. Passage to Cyberactivism: How dynamics of activism change? *Journal of Public Affairs* 3(4): 326-337.

Karatzogianni, A. 2006. *The Politics of Cyberconflict*. New York: Routledge.

Kremer, J. 2014. Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law* 23(3): 220-237.

Matusitz, J. 2008. Cyberterrorism: Postmodern State of Chaos. *Information Security Journal* 17 (4): 179-187.

McCaughey, M. and Ayers, M.D. 2003. *Cyberactivism: Online Activism in Theory and Practice*. New York: Routledge.

Meikle, G. 2002. *Future Active: Media Activism and the Internet*. New York: Routledge.

Pickerill, J. 2003. *Cyberprotest: Environmental Activism*. New York: Manchester University Press.

Savov, V. 2014. Sony Pictures hacked: The full story. http://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream. Accessed January 22, 2015.

Wiemann, G. 2004. Cyberterrorism: How real is the threat? *Special Report No.119*, United States Institute of Peace, December.

—. What's a blackhat hacker? http://www.pctools.com/security-news/hacking/. Accessed February 12, 2015.

CHAPTER TWO

RESISTANCE FROM WITHIN HEGEMONY: THE RISE OF SEMI-ANONYMOUS RESISTANCE IN THE NEW MEDIA ENVIRONMENT

SARPHAN UZUNOĞLU

Introduction

Starting in the 1990s, the Internet became an extraordinarily important means of organizing and constructing political activism on the web. From the Zapatista movement in South America to the protests in Cairo, Tehran and Istanbul, year by year the Internet has been used more effectively by political activists and the structure of political organizations has changed. As in Belarus and Thailand, various countries have regarded the Internet as a political instrument; from election campaigns to surveys, the Internet has been used by political organizations. Yet, the most significant aspect of new media use has been its position within mass movements as a tool for mobilization. Anti-war and anti-globalization movements have used the Internet for communicating within their own groups as well as for promoting their ideas to others. Yet, all these political developments are not limited to NGOs' (Non-Governmental Organizations) or political groups' existence on the Internet. The Internet has changed both the nature of democracy within these groups and activists' methods of protesting all over the world. By scrutinizing the way that anonymity influences in-group practices of democracy and public politics, this article suggests that secure and anonymous new media usage represents a means for replacing existing democratic practices that are maintained under surveillance.

This chapter takes up the conceptualization of anonymity in its various forms because anonymity itself has been a political strategy in both conventional and digital activism in the contemporary world. Newly emerging forms of leaderless and less competitive types of political activism and resistance are analyzed in this study based on the personal

and collective experiences of activists who have used anonymity in various ways for political aims. In addition to proposing that forms of anonymity are instruments for radical democracy, this essay addresses the issues of social conditions and technical layers in order to bring to the surface activists' misperceptions about their levels of anonymity. This study hypothesizes that day by day there are increasing numbers of people who feel that they are threatened by surveillance and try to create measures to oppose it. By drawing on techniques such as pseudonymity and anonymity (protecting personal information on the web), people have started to create individual means of opposing control, and these mechanisms of resistance will be discussed in the following pages.[1]

This essay addresses two dimensions of these reactionary anonymous uses of the Internet. By exploring these dimensions and forms of anonymity, the second part of this study will take up the issue of pseudonymous, semi-anonymous and anonymous users in Turkey's new media environment. The first dimension is referred to here as the technical and theoretical dimension of anonymity, while the second, anonymity, is addressed as a social preference and a method of resistance. In the first part of this study, background information about anonymity and semi-anonymity will be provided, and the various layers and definitions of anonymity will be described. Perceptions and technical methods of providing anonymity will also be discussed in this regard. Those dimensions are based on the social and political experiences of anonymity and its various practices in Turkey's new media environment. In addition, the essay analyses the results of in-depth interviews in terms of the theoretical background. In the conclusion, based on my research I propose that semi-anonymity represents a new way of establishing a radical democratic and secure political network.

Theoretical background of anonymity and semi-anonymity

To begin with, it will be useful to clarify the technical, practical and theoretical definitions of anonymity, semi-anonymity and identifiability. Starting with the layers and conditions of anonymity, I will cover surveillance mechanisms in Turkey's new media environment and the various technical and social methods that have been used to grant anonymity to users. Based on technical and social methods and a theoretical background, I will propose a distinction between anonymity, semi-anonymity and pseudonymity.

Layers and definitions of anonymity

Anonymity is a condition of both users and types of communication, and hence there are various forms and definitions of anonymity. It will be helpful here to briefly discuss the terminology that is used regarding the anonymous use of new media in order to categorize the various forms of anonymity that exist. Naturally, the first of these is anonymity itself. The word "anonymous" is derived from the classical Greek stem *onyma* (name), combined with the prefix a- (the absence or lack of a property) (Clark et al. 2005, 12-13). In short, it is possible to interpret anonymity as the opposite of being identifiable. Baggio and Beldarrain (2011, 2) have noted that "deciding to trust in cyberspace is not without risk, as anonymity protects those who are honest as well as those who intentionally deceive." This suggests that anonymity has both positive and negative connotations. Therefore, being anonymous should be seen not only as a form of resistance, but also as individual or collective action.

Palme and Berglund (2004) state that anonymity is possible when the real author of a message is not indicated and anonymity can be implemented to make it impossible or very difficult to find out the real author of a message. They point out that that anonymity is sometimes thought to be synonymous with pseudonymity, i.e. when a name rather than the real one is visible. Anonymity, however, should not be limited to the protection of detailed data concerning users as the Internet is composed of different structures and in the new media environment people disseminate various types of information about themselves via media applications and networks. According to Hansen et al. (2001, 2) "anonymity is the state of being not identifiable within a set of subjects." They recognized anonymity as a situation in which transmission of a message occurs and they divided it in two different subcategories: sender anonymity, in which a particular message is not linkable to another, and recipient anonymity. In the case of relationship anonymity, it is untraceable who communicates with whom. In other words, the sender and recipient (or recipients in case of a multicast) are unlinkable. Relationship anonymity is weaker than both sender anonymity and recipient anonymity because the person who sends messages may be traceable and it may also be possible to trace who receives messages, as long as the relationship between sender and recipient is not known.

There is an additional set of possible categorizations of layers for defining anonymity. The first is sender and receiver anonymity, the second is connection and message anonymity, the third is the anonymity set and the fourth is unlinkability. In terms of anonymity, this research focuses on these four categories that have been proposed by Joss Wright, Susan

Stepney, John A. Clark and Jeremy Jacob (2005, 14). Hansen et al. (2001, 33-34) initiated a new discussion of other terms such as unlinkability and unobservability, which refer to information hidden within terminology. Also, they argue that the unlinkability of two or more items (e.g., subjects, messages, events, actions, and so on) means that within this system, these items are no more and no less related than they are related concerning a-priori knowledge (Hansen et al. 2002, 1-3). The connection between social media accounts or links between senders of different messages on the Internet can be considered to be a linkability while unobservability may refer to today's coding and encryption technologies by which senders of messages stay completely anonymous but the relationships themselves do not. The terminology mostly depends on the conditions existing in the Web 1.0 environment in which interactivity had not yet penetrated deeply into people's lives. But the terminology they provide can be still used for explaining the "complete" anonymity of relationships in terms of sender-receiver interactions. Accordingly, a sender's anonymity is a precaution taken to protect the relationship's anonymity but for them the recipient's anonymity is another issue that grants anonymity to the relationship.

In the contemporary world, complete anonymity can be considered to be a truly "radical" condition in which relationships are no longer anonymous as receivers are not and observability is higher than ever because of the technologies mentioned above. The relationship's observability is based on technical applications such as dummy traffic, steganography, which can be defined as hiding messages in a way that cannot be detected, and a spread spectrum (Hansen et al. 2002, 5).

The technical- and interaction-based definitions of the term "anonymity"' provide users with certain advantages. For instance anonymity allows for the masking of handicaps and accentuating certain individual characteristics, which might lower inhibition (Döring 2003, 460). One can create an identity for oneself free of all biases and legal constrains within society. Fuchs (2008, 322) states "anonymous identity is not free from the social past of a human being as social experiences and the individual history of an individual influence and shape his or her online behaviour."

Social and technical methods used for anonymity

Software and other technological means can be used for a user to remain anonymous. The first focus point of anonymity is dividing social networks from one another. Someone who desires to be anonymous will generally create new aliases because a large number of aliases makes it more difficult to pinpoint the identity of the individual. For local security