ABSTRACT

Title of dissertation: HACKING FOR DEMOCRACY: A STUDY OF THE INTERNET AS A POLITICAL FORCE AND ITS REPRESENTATION IN THE MAINSTREAM MEDIA

Sandor Vegh, Doctor of Philosophy, 2003

Dissertation directed by: Professor Myron O. Lounsbury
Department of American Studies

The purpose of this dissertation is to understand the politics of the Internet and its impact on democracy and democratization, online political activism (hacktivism), the hacking phenomenon and the discourse around it, as well as the media’s role in this discourse. In particular, it provides a thorough analysis of the media representation of hackers, hacking, hacktivism, and cyberterrorism.

This dissertation examines the mainstream mass media coverage of the political uses of the Internet in a larger theoretical framework of an online hegemonic power struggle between the elite and the public. In order to better understand this process, I construct a model to classify the online forms and actions of control and resistance that have an impact on democracy and democratization. The central questions to which I seek answers are how democratizing or undemocratizing these activities are, and what role the media play in the process.

Especially after September 11, 2001, the national debate on the security of cyberspace has intensified. It has negatively influenced the movement of online political activism, which is now forced to defend itself against being labeled by the authorities as a form of cyberterrorism.
However, these socially or politically progressive activities often remain unknown to the public, or if reported, they are presented in a negative light in the mass media.

In support of that claim, I analyze five major U.S. newspapers in a one-year period with 9-11 in the middle. I argue that certain online activities are appropriated for the goals of the political and corporate elite with the help of the mass media under their control to serve as pretext for interventions to preserve the status quo. Thus, the media portrayal of hacking becomes part of the elite’s hegemony to form a popular consensus in a way that supports the elite’s crusade under different pretexts to eradicate hacking, an activity that may potentially threaten the dominant order.
HACKING FOR DEMOCRACY:
A STUDY OF THE INTERNET AS A POLITICAL FORCE AND ITS REPRESENTATION IN
THE MAINSTREAM MEDIA

by

Sandor Vegh

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2003

Advisory Committee:

Professor Myron O. Lounsbury, Chair/Advisor
Professor Mary Corbin Sies
Professor John L. Caughey
Professor Ray E. Hiebert
Professor John E. Newhagen
# TABLE OF CONTENTS

PREFACE ........................................................................................................................... ii  
ACKNOWLEDGEMENTS .............................................................................................. vii  
LIST OF TABLES .............................................................................................................. x  
LIST OF FIGURES ........................................................................................................... xi  
CHAPTER 1: INTRODUCTION ....................................................................................... 1  
   Overview ......................................................................................................................... 1  
   Society, power, and the media ........................................................................................ 7  
   Historical theories of the press ...................................................................................... 10  
   Domination theories ...................................................................................................... 19  
   Media ownership ........................................................................................................... 26  
   Theories of the new media ............................................................................................ 30  
   Research methodology .................................................................................................. 34  
CHAPTER 2: THE INTERNET AND DEMOCRACY IN WESTERN SOCIETIES .... 40  
   Democracy .................................................................................................................... 42  
   ICTs and democracy ..................................................................................................... 46  
CHAPTER 3: THE INTERNET’S ROLE IN DEMOCRATIZATION ....................... 65  
   The democratization process ......................................................................................... 66  
   The Internet as a democratizing force ........................................................................... 69  
   The democratization of the Internet itself ..................................................................... 71  
   Studies on the Internet and democratization ................................................................. 75  
CHAPTER 4: CONTROL ................................................................................................ 88  
   Defining control ............................................................................................................ 88  
   Censorship ..................................................................................................................... 95  
   Surveillance ................................................................................................................. 103  
   Propaganda .................................................................................................................. 111  
   Containment ............................................................................................................... 115  
   Shifting alliances ......................................................................................................... 124  
CHAPTER 5: RESISTANCE ......................................................................................... 129  
   Defining resistance ...................................................................................................... 129  
   Privacy protection ....................................................................................................... 133  
   Alternative news sources ............................................................................................ 138  
   Online advocacy .......................................................................................................... 144  
CHAPTER 6: FROM HACKERS TO CYBER WARRIORS ....................................... 151  
   Hacking ....................................................................................................................... 151  
   Cyberwar ...................................................................................................................... 168  
CHAPTER 7: CYBERACTIVISM ................................................................................. 176  
   Forms of online political activism ................................................................................ 176  
   Examples of online political activism ........................................................................... 181  
   Cyberprotests against the World Bank ........................................................................ 196  
CHAPTER 8: HACKTIVISM AND THE MEDIA .................................................... 207  
   Shift in the national discourse on hacktivism ............................................................. 207  
   Academic discourse on the media image of hackers ................................................. 224  
   The media’s role in the portrayal of the Internet as a political force ...................... 228
Overview

Power struggle between the haves and have-nots has been an integral and crucial part of the history of humankind since people organized themselves into societies. Starting as early as the Hellenic Age formations of statehood based on concepts such as democracy and protected rights held the first promises to social reconciliation. In the Modern Age the ownership of the means of production has been in the center of social tensions. In the early 20th century technological advancement and mass production brought about new hopes for the average people in terms of availability of mass consumer goods. Cars, radios, telephones, and television sets have offered new ways of freedom in transportation and communication. Like every new technology, freedom comes at a price and is not available for everyone. Arguably the greatest of such promises in recent times, the Internet is no exception. After the initial euphoria about its democratic potentials it became yet another site of contest. Like most other communication technologies, the Internet turned out to be a means of control and resistance at the same time.

On the one hand, it is another medium to disseminate information favorable to those in power, another communication channel that can be regulated and monitored, and another platform for continuing what capitalism does best: sell. On the other hand, the Internet is a tool in the hands of those privileged enough to have Internet access to acquire news and information from alternative sources, to voice their opinions and offer personal interpretations of events, to circumvent censorship by their governments, and to confront the authorities imposing the sanctions.
Ideologies and tools of online control are naturally different in democratic and non-democratic countries. While democratic principles and economic profit seem to happily co-exist regarding the Internet, they are fighting their covert battles in both worlds. For the elite\(^1\) this fight is aimed at achieving control online, for the masses, it is a fight to keep the promise of the Internet as a new public sphere, open to everyone and free from political and commercial control. For the elite, the subversive/liberating power of this new technology must be contained at all costs. For the public, privacy of communication, freedom of information, universal access, genuine diversity of opinions, and true democracy must be protected.

I will further elaborate on the interaction of political forces shaping the Internet by describing a three-actor model that symbolizes the hegemonic power struggle among the government, the corporations, and the public. The major driving forces behind these actors are national security, corporate interest, and civil liberties, respectively. Yet, this is not just a fight for the particular interest of these actors, but also a reconciliation dilemma, since all of them realize the right to personal privacy, the need for business policy and development, and law enforcement for public safety and national security. The question is to what extent each should unfold at the expense of the others.

Once an alliance is established between the government and the corporate world, these online control and resistance activities can be framed as a dialectical power struggle between the elite and the public. We may look at this control and resistance struggle as the thesis and antithesis of domination on the Internet and for the Internet. Yet, as the Chief Executive Officer of Hewlett-Packard noted in her speech surprisingly set on a Hegelian track, “from a contradiction and conflict arises a true synthesis that unifies these different views into a

\(^1\) The elite refers to the dominant powers in society that include the corporations, global financial institutions, traditional interest groups, major parties, the government, and upper-class influential societal figures usually associated with any of the previous entities.
cohesive, and often unexpected, understanding” (Fiorina, 2001). The connections between these polar opposites lie in the underlying technologies that both utilize in their struggle of control and resistance. Whereas we cannot accept absolute understanding between the opposites, there is a synthesis that promises a balanced approach to the Internet, until a new development does disturb the status quo again. One such development that, in fact, upset the status quo and gave way to a new synthesis at the same time was what later turned out to be a central theme of this dissertation: the tragic events of September 11, 2001.

In Chapter One, I will map the current state of mainstream scholarship exploring the connection of democracy and the Internet. I will show that there are two main trends: one that concentrates on the traditional institutions and processes of democracy and examines where the Internet can contribute (e-democracy, e-governance), and another one that seeks the newly emerging ways how the Internet may alter or influence democracies and the process of democratization. This latter approach includes the study of non-traditional and oppositional online activities that may be deemed undemocratic in one country, but democratizing in another one.

Chapter Two will shift the focus to these activities, namely, how the Internet helps or hinders the process of democratization. This chapter prepares the ground for answering the call by several scholars for more research into the Internet’s democratic role in different countries, and how dissent groups and opposition movements use the Internet to criticize the authorities and mobilize support.

In Chapter Three, I will systematically survey the tools and ways of domination online. The perils and potentials of the Internet have been realized by governments equally from non-
democratic to fully democratic societies. However, the undemocratic practices regarding the Internet are not limited to non-democratic regimes; we can identify several attempts in advanced Western societies to monitor, limit, or control personal communication or information-seeking procedures. When their information monopoly is threatened, corporations and governments react by spreading online propaganda, imposing surveillance mechanisms, or exercising censorship. These overt or covert tools of control will be categorized into four types: *censorship*, *surveillance*, *containment*, and *propaganda*.

Chapter Four is basically the antithesis of Chapter Three; it explores and categorizes online resistance, the ways in which control is defied, censorship is circumvented, private communication and information is protected, protest movements are organized, and direct action is carried out. These online activities range from constructive Web site postings to destructive server hackings. Online resistance will be mapped into five categories: *privacy protection*, *alternative news*, *online advocacy*, *hacktivism*, and *cyberwar*.

Having constructed a theoretical framework, mapped out the related online activities, and situated cyberactivism, I will concentrate on one particular form of online resistance: hacktivism. To establish the foundation, Chapter Five will deal in depth with the concept of hacking as the underlying act in many forms of hacktivism. In Chapter Six, I will analyze and classify the forms of online activism, followed by examples to show the diversity of these activities, regardless of their political cause or geographic location, and provide a system for understanding various forms of online activism. It will be followed by a case study in which I will examine how the online aspects of the anti-globalization protests against the World Bank fall into this classification system. I will pay particular attention to the forms and results of online dissent.
preferred by the activists, as well as to the strategies the Bank deploys to handle these cyberprotests.

Finally, Chapter Seven will put hacktivism in the center. I will review the academic discourse around hacktivism, analyze the different perspectives on it, including that of the academia, the government, the military, the Internet security industry, and the public. However, these socially or politically progressive activities often remain unknown to the public, or if reported they are presented in a negative light in the mass media. In the same chapter, I will provide evidence to this claim, and reveal the operating political or commercial forces that shape the presentation of these activities in the mainstream mass media. Furthermore, it will also be argued that preventive or counter measures on the Internet by those in power are not reported, or they are framed in a way that is most likely to receive public support.

To achieve its political and commercial goals, the U.S. administration needs public support. Therefore, as I theorized, the government will exercise its utmost influence to have the media present these events in a light that is favorable to its interest. Given the intricate ties between corporate interest, media ownership, and American foreign policy, this task is fairly easily achievable. Just to give a classic example, American foreign policy decides on wars, which require arms that are supplied by major military contractors who, in turn, are also owners of media companies that, in turn, set the public agenda and influence the people’s opinion, which determines the support of the government and its foreign policy.

In Chapter Seven, I will give support to the argument on the biased media language regarding hacking and online political activism. I will expose if and how the tone and perspective of reporting have changed as a result of the terrorist events of September 11, 2001. In particular, I will put hacktivism into political and legal context, review the relevant scholarly studies, and
analyze the language of selected sources for clues in their discourse of hacktivism and cyberterrorism. These sources consist of articles from major U.S. daily newspapers, such as the Washington Post, the New York Times, USA Today, and the San Jose Mercury News, as well as wire services reports and a few other relevant news sources, such as the Computerworld magazine. In this chapter, I will focus on official government documents, while in the next chapter, news media reports will be put under the microscope.

The main contribution to new knowledge comes in Chapter Eight that contains the quantitative research that supports my earlier observations of the tendencies in news media portrayal of hackers and hacking, especially post-September 11. In this chapter, I conduct a content analysis of five major U.S. newspapers over a one-year period. Furthermore, I include the outcome of two additional research projects, namely, about the media use of cyberactivism and cyberterrorism in the context of the focal concepts of this chapter: hacking and hackers.