NETWORKS OF RESISTANCE:

ONLINE ACTIVISM IN THE INFORMATION AGE

by

David Kim Juniper

B.A., Concordia University, 1993
Dip. Ed., McGill University, 1995

THESIS SUBMITTED IN PARTIAL FULFILLMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

in

INTERDISCIPLINARY STUDIES

THE UNIVERSITY OF NORTHERN BRITISH COLUMBIA

March 2000

Abstract

The purpose of this thesis is to show how the anarchistic structure of computer-mediated communications networks empowers small activist cells by allowing them to circumvent established informational structures and establish highly flexible and dynamic "webs" of cooperation and support. The rise of these new modes of communication was significant for it enabled online activists to bypass established media such as television and newspapers and disseminate information directly to a mass audience. Through an analysis of online culture and the growth of the social netwar waged by the Zapatista of southwest Mexico, I suggest that the Internet and its use by online activists had a significant impact on the rebellion and is influencing the Mexican government to seek a negotiated settlement as opposed to a military solution to the conflict. The research design involves a review of a wide variety of literature on the topic, including academic journal articles and scholarly works as well as popular magazines and electronic mailing lists. Because of the nature of the research, much of the material came from online sources such as world wide web sites, electronic mailing lists and gopher sites. Inquiries of this kind into the nature of Internet culture are important if we are to understand the implications and impacts of the Internet on the political fabric of Western society. We are in the midst of the digital age, and academic study is of paramount importance if we are to understand not just where we are, but where we are headed.

TABLE OF CONTENTS

Acknowledgements

I wish to thank, first and foremost, my wife Paylig for without her continued support, patience, understanding, strength, good humor and insight I would never have come this far. *Hazar shnorhagaloutiunner!*

Thanks to Lynda Willliams, Project Leader at the Centre for Teaching and Learning, for her continued support, encouragement and enthusiasm. You're the best, Lynda!

Thanks to my committee members, Dr. Heather Smith, Dr. Antonia Mills and Dr. Tracy Summerville for the insightful comments, careful readings of my work and lively committee meetings. Likewise, my thanks go to Dr. David Casperson for his keen and helpful comments and suggestions during my thesis defense.

And finally, thanks to the netwarriors who, despite often overwhelming odds, continue to fight for human rights in all countries of the world. May the flame never die, and the spirit never falter.

...technology is changing the equations of power, challenging the conventional channels of communication, distributing and disseminating influence in the broadest possible fashion, to the point of democratizing the channels and getting rid of the gatekeeper.... The technology has a mind-boggling potential to break through barriers and overcome political obstacles to educate, inform and be an agent of political change....The mouse is mightier than the missile.

-- Lloyd Axworthy, Canadian Minister for
Foreign Affairs and International Trade

Introduction

In a work entitled Electric Language, Eric McLuhan suggests the mythological Arachne as the best representation of the rebellious spirit of much of online culture (1998). A young girl born in the town of Idmon of Colophon, Arachne was a peasant girl gifted with an incredible skill as a weaver. This talent, a gift from the goddess Athena, quickly brought the girl fame and renown throughout Greece. All day she wove her cloth to the wonder and amazement of all that beheld her, and so famous did she become that even great Athena, goddess of arts and crafts, grew jealous. Upon hearing that Arachne had claimed herself to be a better weaver than the goddess, Athena descended to earth and challenged the mortal girl to a contest. Undaunted, Arachne agreed and began to weave.

> Each competitor worked feverishly at the loom, spinning and weaving their masterpieces. Nonstop work, fingers and feet flying, an incredible sight for all watching. The two seemed to tune out the world and the universe, concentrating on their tapestry and the story that it may tell. Athena finished her work, and held up the incredible piece of work. The tapestry told the story of Athena and Poseidon, in their battle for control of Athens…
>
> …Arachne then held up her piece, the foolish mortal wove various stories of the gods' less honorable victories. Some of the scenes included such things as gods deceiving women and other goddesses, making fools out of the gods. The tapestry was clearly an attempt of mockery and shame for the gods... Athena quickly became angered, looking for fault in the girl's work. She searched the tapestry up and down, left and right, but could not find a fault anywhere. Athena called upon Envy to search Arachne's work, and yet even the great Envy could find not a single thread out of alignment. Athena's rage took hold of her, jumping towards Arachne with the wooden shuttle in her hand, repeatedly beating her face in with the tool… (Zaferakis 1998: n.pag.)

Still defiant, Arachne escaped the wrath of the defeated goddess by hanging herself. In death her form altered and she became a spider, a weaver still, and mother to countless descendants. Free from Athena's fury, Arachne's brood spread their webs

around the globe trapping the unwary and amazing all with their beauty, complexity and ruthless efficiency.

Like Arachne, online activists first learned to weave network webs from a major military power, the American military, through a project known as the Advanced Research Projects Agency (ARPA). The technology quickly spread beyond the walls of ARPA, until computer-mediated communication (CMC) was no longer under state control but had become a world unto its own. Like Athena, governments flexed their muscles and brought down their swords, but have not been able to control what they themselves have created. As a result, the net, also known as the matrix, cyberspace or cyberia, has captured the imagination of activists worldwide, and has become a source of deep concern for both governments and corporations.

But what is cyberspace? According to Dan Thu Nguyen and Jon Alexander, cyberspace denotes a "polymorphous reality" where CMC occurs, a space where physicality no longer matters, and architecture is liquid (Nguyen and Alexander 1996, Novak 1992). First introduced by author William Gibson in the early eighties, the term *cyberspace* embodies a digital realm where the body is superfluous and the mind melds into vast seas of binary data. Cyberspace surfers can communicate, share documents including audio and video files with others around the world, thereby creating a communications network largely independent from government censorship and control (Shields 1996). The structures of computer-mediated communications offer small, semi-independent activist cells the opportunity to form flexible, acephalous networks of resistance, giving them an organizational and informational advantage over more rigid, hierarchical organizations such as militaries and governments.

The purpose of this thesis is to show how the anarchistic structure of cyberspatial networks empowers small activist cells by allowing them to circumvent established

informational structures and establish rizomatic "webs" of cooperation and support. It is delivered from the activist perspective, thereby emphasizing elements such as freedom of speech, unfettered communication, and the advantages presented by rizomatic network structures. One of the major assumptions underlying this work is that in order for political discourse to flourish online, there must be little or no control over what topics can or cannot be discussed over the Internet. Government censorship of online content that does not break the civil or criminal code is perceived in this thesis as an attempt by the state to overextend its influence into the online sphere, possibly for political reasons. For this reason, because of recent actions on the part of Western governments to gain excessive control over the Internet, the state is treated as a potential threat to the freedom of expression online that is vital to online political discourse. This is not to say that cyberspace should become a haven for criminals, however. Law-breakers online, as offline, should be ready to face the legal consequences of their actions (for example, uttering death threats is an offense online or off). Efforts on the part of the state to extend censorship over the online medium and affect those who have broken no laws, in effect censoring speech rather than action, will be treated as a threat to online activists. This discussion will involve a brief overview of recent attempts at censorship on the part of the US government, and will be supported by both Libertarian as well as anarchist theory.

For the purposes of study, in this thesis I have concentrated on groups involved primarily with the Zapatista in particular and with human rights in general, yet the potential of the Internet as a conduit for political struggle is not limited to those groups. Environmentalists, Marxist revolutionaries, white-power extremists as well military and intelligence agencies can and have employed online strategies as part of their individual campaigns. As a medium for the sharing of information and propaganda, therefore, the

Internet is open to all. However, as we will see, the effectiveness of a given netwar is greatly dependant upon the ability of a group to garner popular support. The secret of the Zapatista success was their ability to communicate in such a way as to gain support from many different people, from labor groups to academics to students. For alternative online actors such as neo-nazis to fight a netwar would arguably be much more difficult, for they would have to overcome popular opposition in their quest for support. Such groups may be more likely to resort to aggressive hacktivist tactics rather than the softer netwar approach. Although hacktivism was also used by supporters of the Zapatista, these tactics garnered severe criticism from many Zapatista supporters and were not part of the main Zapatista netwar.

I will summarize the contents of the chapters here.

Chapter 1

Chapter one describes the principal theoretical structure within which this thesis unfolds, providing a clear definition of soft power, and offering a discussion of the nature of information. Unlike chapters 3, 4, and 5, which describe the political persuasions of various actors involved in information wars, this section deals with the political structure of the matrix itself. At the outset of the chapter, a discussion of the nature of information will provide a basis upon which to build the case for information warfare as a viable alternative for political activists. Citing works by Murray Bookchin, William Godwin and others, it will define anarchy and demonstrate how many of its fundamental theoretical underpinnings permeate much of contemporary online culture. This discussion will provide the basis for further debate on such issues as rizomatic activist networks vs. traditional hierarchical structures, achieving speed and flexibility on the matrix, as well as the importance of freedom of expression and privacy online.

Chapter 1 will also introduce the concept of *soft power* and how it has become a major power in the hands of wired activists as well as state and corporate actors. Unlike 'hard' power that targets the body of the opponent, soft power affects the foe psychologically. Through its strategic use, an opponent can be subtly coerced into adopting a desired course of action without the threat of physical violence being necessary. The importance of soft power online is vital to the understanding of informational warfare, for it not only empowers activists but can also become a formidable weapon in the hands of the military and intelligence agencies. Through a sound understanding of soft power, an appreciation can be achieved both for the possibilities and the perils of information warfare.

Chapter 2

In the beginning of chapter two, the origins of ARPAnet will be explored, outlining the motivations and significant events involved in the creation of what would later be termed "cyberspace." The different communications protocols used on the matrix will be defined, and their respective strengths and weaknesses assessed for use in later discussions. Understanding the beginnings of cyberculture is important for it is at this point that the seeds of rebellion were sown which would later fuel much of the action surrounding the Zapatista netwar. The main sources for this section are Rheingold (1993) and Sterling (1993). The chapter will deal with a study of the growth of Unix and its role in the democratization of the matrix, highlighting the public nature of the operating system's source code as a major factor in the spread of computer-mediated communication beyond the borders of ARPAnet. This will be followed by a look at Bulletin Board Systems and issues of online freedom. The chapter will close with a look at the growing potential of the World Wide Web as a networking tool.

Chapter 3

Information warfare, referred to as netwar by RAND analysts John Arquilla and David Ronfelt (1997), will enter the scene in chapter three. As a military strategy, netwar offers a paradigm in which soft power becomes the prime weapon in a battle to sway public opinion and/or undermine the socio-political beliefs of the enemy. Unlike hacktivism, which involves the aggressive use of hacking skills in attacking the opponent's information structure, information warfare is the dissemination of information as part of a soft power strategy. Taking examples from, among others, the Zapatista netwar, this new merger of the hacker and the activist will be exposed and presented as constituting a new chapter in this rapidly emerging field. The debate amongst wired activists regarding the merits of hacktivism will also be highlighted as an example of the many differing views on existence in cyberspace, a debate that can be expected to intensify as more activists turn to the matrix as part of their strategy.

Chapter 4

Chapter four explores the close relationship between the governmental, military and intelligence agencies with regards to command, control, communications, computers & intelligence (C4I). Through a discussion of Libertarianism and its relationship to the US government's attempts to suppress free speech and extend its influence over the Internet, an argument will be offered for the maintaining of free speech online. The relevance of this chapter to the case study involves the belief that in order for the Zapatista netwar to continue successfully its participants must remain aware of the dangers from both the state and military spheres. Although the online experience combined with cyborgian sensibilities tends to foster a sense of empowerment and quasi-invincibility in wired activists, it must be underlined that the state is no longer a

stranger online and is in fact extending its power into the digital realm. In order to place the state's growing interest in the matrix in an historical context, an overview of the long-standing fear of potential attacks by invisible "information warriors" on the national and international communications grid is highlighted. The chapter then deals with military and state perspectives on online security, drawing links between these and the actions of militant hacktivists described in the previous chapter.

The unveiling of Echelon, a complex communications monitoring system involving five countries and targeting primarily civilian telephone, fax, telex and email communications, will provide proof of the international intelligence community's concerns and skill in using the matrix as a vast surveillance network. The main document supporting this section will be a study presented to the European Parliament in January, 1998, entitled An Appraisal of Technologies for Political Control, written by Steve Wright of the Omega Foundation- Manchester. Combined with American and British newspaper and magazine articles, this section aims to reveal how intelligence agencies around the globe possess the ability to monitor all forms of electronic communication.

Chapter 5

"The Zapatista Netwar" constitutes my case study and reveals the anatomy of a netwar currently being waged across the ether by a web of activist groups across the world. It begins with an historical description of Chiapas, a province in southeastern Mexico. Quoting a Human Rights Watch report as well the writings of John Collier (1994) and Subcomandante Marcos (1994), the poverty and violence characterizing life in the province is exposed and set as a backdrop for the Zapatista revolution. Of note will be the influence exercised by Chiapan Catholic and Protestant churches in the raising of indigenous awareness and pride, as well as their role in creating the first

contemporary networks of resistance amongst scattered indigenous villages.

The analysis of the movement itself, from 1994 to the present, will emphasize the differences between it and previous guerrilla movements and how these differences contributed to making their insurgency well suited for the global digital stage. Using studies from the RAND Corporation, the writings of Cleaver, existing interviews and communiqués by Subcomandante Marcos as well as eye-witness testimonials from members of NGOs and Zapatistas themselves, a portrait will be offered of how the Zapatistas became Mexico's first "post-modern warriors." Taking the writings of Von Clausewitz (1976) on war as well as perspectives by Szafranski and Arquilla (1997), the Zapatista social netwar strategy is described and its effectiveness accessed with regards to winning concessions from the Mexican state. To suggest the effectiveness of the Zapatista Internet campaign, statistics regarding worldwide coordinated demonstrations following the massacre at Acteal in December of 1988 are quoted and assessed. The chapter ends with a discussion of the major actors involved in the social netwar as well their individual roles in turning a local, indigenous uprising into a global campaign described by Cleaver as the "Zapatista Effect."

Beginning with the rise of computer-mediated communication and closing with a description of the Zapatista netwar, this thesis offers a look at the growing phenomenon of online activism. Through an analysis of the flexible, unhierarchical and anarchistic nature of the medium, a hypothesis is formulated as to why this medium provides an effective environment for the waging of social and political activism and examples are offered in support of this hypothesis. Through an analysis of the activities of intelligence agencies online, the pitfalls facing social activists in cyberspace are revealed. The Zapatista netwar, an example of a contemporary netwar currently being waged across the matrix, will close the thesis. Showing how through the matrix the Zapatista created a

web of international supporters who helped pressure the Mexican government into seeking a negotiated settlement with the Zapatista, the case study will suggest that netwars are effective and should be considered an integral part of the general social activist strategy.

Chapter 1

Information, Anarchy & Soft Power

1.1 Introduction

As any well-planned voyage requires a detailed map, this study necessitates a sound theoretical framework within which to unfold. In order to assist in the navigation of these digital waters, the theoretical approaches employed require a high level of flexibility and adaptability, for they would be required to operate "outside of the box" of traditional theory. The main themes addressed in this chapter are the nature of information, the meaning of hierarchy as related to the structure of online networks of resistance and the importance of heterogeneity within the digital sphere. These concepts are approached primarily through anarchist writings that underline the perils of central authority. According to Peter Kropotkin, anarchism is defined as

> the name given to a principle or theory of life and conduct under which society is conceived without government- harmony in such a society being obtained, not by submission to law, or by obedience to any authority, but by free agreement concluded between the various groups, territorial and professional, freely constituted for the sake of production and consumption, as also for the satisfaction of the infinite variety of needs and aspirations of a civilized being. (Qtd. In Shatz 1972: xi)

Placed in the cyberspatial context, anarchy provides the foundation upon which to explore netwar and establish the factors involved in pursuing an effective online campaign. This is not to suggest that the Internet is part of a worldwide anarchist movement or that the medium somehow promotes a transition to anarchy, but to suggest that the physical and societal structure of the medium is best represented through the anarchist model. Due to a lack, at the present time, of any central authority, the Internet serves as home to peoples of all political persuasions, from the capitalist to the socialist to the indigenist. Thus providing the environment for the flowering of political discourse, the anarchistic system acts as a vehicle for freedom of expression but, in itself, imposes

few constraint upon what such expression would be.

The concepts of information, hierarchy and soft power will be introduced as a triad upon which the thesis will stand. Under the banner of information, the themes of control and coordination are highlighted as core concepts in understanding the principal opposing strategies on the digital battlefield. The themes introduced in this discussion are further examined in the hierarchy section, which explores the meaning of hierarchy online and its significance to digital conflict. As opposed to the Marxian perspective of hierarchy where class conflict occupies center stage, the perspective on hierarchy outlined in this section deals with the social and physical structure of the network as a whole. Contrasting hierarchical structures as top-down power systems with the un-hierarchical acephalous webs of semi-independent actors, this section emphasizes how the speed and flexibility of online activists are major tactical advantages in this new field. Closing with a discussion on soft power, a strategy targeting the mind of the opponent and the potential ally as a way of achieving victory, this chapter will lay the groundwork upon which the following chapters will build.

1.2 Information

For the purposes of this thesis, we will focus on the medium across which information travels (Arquilla & Ronfelt 1997). In a cyberspatial context, this perspective would consider the acephalous nature of the network system, the flexibility of electronic mail, and the inherent power of the mailing list. Followers of this approach generally adopt a highly structured approach, perceiving that without order, information cannot be propagated. During the 1940s and 1950s, most research in this field was dedicated to the study of control as the ideal strategy for maintaining a structured system or society (Arquilla & Ronfelt 1997: 147). Control, it was believed, was necessary to maintain an order within which information can easily spread. Recent research, however, suggests that *coordination*, a more decentralized, flexible approach, may be but the flip side of the

"order coin".

> Control and coordination are different, sometimes contrary processes; indeed, the exertion of excessive control in order to avoid entropy may inhibit the looser, decentralized types of coordination that often characterize advanced forms of complex systems. (Arquilla & Ronfelt 1997: 148).

Although both of these approaches agree that in order for information to circulate structure must be present, *control* and *coordination* assume very different strategies in achieving and maintaining the optimum informational environment. As the rest of this thesis will suggest, within CMC *coordination* constitutes the most efficient approach for the sharing of information, and in so doing constitutes a profound challenge to actors used to *control* strategies.

1.3 Hierarchy

In our contrast of *control* vs. *coordination*, one of the principal issues is the relationship between hierarchal structures and the wielding of power online. Anarchist writer Murray Bookchin rejects *control* as a dominant informational paradigm, preferring instead the fluid and rizomatic *coordination* as an organizational theory (Bookchin 1991: 4). The un-hierarchical nature of much online strategy is emphasized by RAND analysts John Arquilla and David Ronfelt in their groundbreaking essay "Cyberwar is Coming" (1997). As a child of the digital, or "information," revolution, the matrix embodies many of the hallmarks of the new age from which it sprang. In a discussion of the impacts of what Alvin Toffler termed "The Third Wave" upon industrial-era institutional structures, Arquilla and Ronfelt note how,

> [t]he information revolution, in both its technological and non-technological aspects, sets in motion forces that challenge the design of many institutions. It disrupts and erodes the hierarchies around which institutions are normally designed. It diffuses and redistributes power, often to the benefit of what may be considered weaker, smaller actors. It crosses borders and redraws the boundary of offices and responsibilities… The network form is very different from the institutional form. While institutions (large ones in particular) are traditionally built

> around hierarchies and aim to act on their own, multi-organizational networks consist of (often small) organizations or parts of institutions that have linked together to act jointly. The information revolution favors the growth of such networks by making it possible for diverse, dispersed actors to communicate, consult, coordinate, and operate together across greater distances and on the basis of more and better information than ever before. (Arquilla & Ronfelt 1997: 26-7)

In an essay entitled "The Zapatistas and the Electronic Fabric of Struggle," Harry Cleaver described the ways in which the network's non-hierarchical form functioned in the course of the Zapatista netwar. Therein, Cleaver shows how a collection of loosely connected individuals working towards human rights in Chiapas coalesced into a highly networked international web through which information and calls for actions circulated quickly and efficiently. Although lacking any central organizing authority as would exist in a hierarchical system, these early netwarriors worked together to spark and respond to what would become a global struggle both on and off-line.

> As the number of people involved in these processes of uploading, re-posting, translating, etc.[sic] has grown, so has their self organization. What began as, and to a degree still is, an interlinked set of spontaneous actions has become more organized. On some lists, for example, a cooperative division of labor has emerged so that a dozen or more people take individual responsibility for tapping and reposting relevant material from particular sources to a single site in cyberspace.(27) In this way the skills and resources of many separate individuals and computer systems are connected in ways that benefit everyone tapping the pooled information. In another case, the best material from a few such poolings is reposted to those who need the information but don't have time to search out even a reduced number of sites.(28) As a result of such co-operation, the work of culling The Net has been drastically reduced for the vast majority of those needing and using information about the struggles in Mexico for purposes of mobilization and solidarity. (Cleaver 1995: n. pag.)

1.4 Soft Power

Soft power, unlike hard power, affects the mind of the target (Barber 1995). In the realm of advertising, for example, this may involve convincing people that to drink a given soft drink will give them an aura of youth, dynamism and sexual attractiveness.. At best, soft power works without the target being aware that he/she is being influenced, resulting in an unconscious defeat and a silent victory.

In eighteenth century England, William Godwin warned his readers of the treachery of soft power and called for vigilance in the face of a state that he believed was the prime antagonist and wielder of this subtle weapon:

> Perhaps government is, not merely in some cases the defender, and in other the treacherous foe of the domestic virtues. Perhaps it insinuates itself into our personal dispositions, and insensibly communicates its own spirit to our private transactions. (Godwin 1793: 7).

Joseph Nye has written extensively on the use of soft power by states in the international arena, showing this strategy has applications both within and outside of the domestic realm. In an essay entitled "Soft Power," Nye discusses the nature of this new strategy and its role in the changing international scene.

> ... political leaders and philosophers have long understood the power of attractive ideas or the ability to set the political agenda and determine the framework of the debate in a way that shapes others' preferences. The ability to affect what other countries want tends to be associated with intangible power resources such as culture, ideology, and institutions. (1994: 138).

Richard Szafranski describes politics as the "pursuit and exercise of power," and 'power' as "the ability to influence people who otherwise might not choose to be influenced." (1997: 397). Following these definitions, therefore, one can see how soft power can be used as a subtle political alternative to such methods as media control, coercion, threats and blackmail. In contrast to "hard" warfare, a well-implemented strategy using soft power allows the protagonist to choose the battlefield and vanquish the foe without the foe ever realizing what a battle has even occurred. As Szafranski discusses,

> The object of war is, quite simply, to force or encourage the enemy to make what you assert is a better choice, or to choose what *you* desire the enemy to choose. Said another way, the object of war is to subdue the hostile will of the enemy ... if the object of war truly is to *subdue hostile will* or *to make the opponent comply with our will*, then we must consider enemies not just as systems, but as organisms with will. Likewise, if weapons are *means used to coerce an adversary's will*, then even our understanding of weapons must go beyond things, implements or tools. (1997: 397)

In an online essay entitled "Canada and Human Security: the Need for Leadership," Canadian Foreign Minister Lloyd Axworthy discusses the nature of soft power and its role in the international arena.

> Soft power is the art of disseminating information in such a way that desirable outcomes are achieved through persuasion rather than coercion. Because it sets the terms of the debate, soft power influences the nature of the solution. It blurs, even counters, the perception of traditional power assets, such as military force, economic might, resources, and population. Power in this context is obtained from networking and coalition-building. To wield soft power will require a mastery of information technologies to ensure that Canada has a superior knowledge base. The government will have to call on all of the resources at its disposal to manage information and to develop innovative foreign policy tools. (Can. Dept. of Foreign Affairs 1998: n. pag.)

Axworthy continues by noting how powerful an actor's international image is when using soft power. The Zapatista, who carefully tailored their political message in order to appeal to as wide and heterogeneous an audience as possible, understood the importance of public relations skills and used it to great effectiveness in their campaign against the Mexican state. Although the Minister deals specifically with the use of soft power by Canada, the same can be said of any actor pursuing a soft power strategy.

> A country's image is key to the use of soft power. An attractive set of values and an image as a trustworthy partner encourage other countries to consider and weigh our views. In a soft power context, Canada benefits from its status as an open, industrialized society where citizens enjoy a high quality of life and protection of their human rights. Canada also benefits from its vibrant multicultural society. But to secure the maximum benefit from these assets, Canada must consider how to promote its values and culture more widely abroad through a more comprehensive international information programme... The increasing availability of information technology will fundamentally alter the international political landscape. It has already linked much of the world together as a global commons and will, to paraphrase Marshall McLuhan, transform the world as dramatically as Gutenberg's press did in the Middle Ages. (Can. Dept. of Foreign Affairs 1998: n. pag.)

It is this ability to "promote its values and culture more widely abroad through a more comprehensive international information programme" which is the mark of the superior info-warrior. By effectively convincing others to subscribe to its perspective and/or point-

of-view, the skilled info-warrior can gather public support while simultaneously eroding the enemy's power base, perhaps even undermining the enemy's confidence in its own position.

John Rothrock, director of the Center for Global Strategic Planning at the Stanford Research Institute International, emphasizes that information warfare involves very different approaches from traditional 'hard' warfare, and the impacts of this strategy as well may be very different from what one would expect (1997: 227). Only through a deep understanding of the enemy's cultural, social and psychological make-up can successful information warfare be waged, and likewise only through mastery of the medium can the effects of the strategy be controlled and exploited to best advantage.

Considering the nature of the matrix, the lack of a clearly defined "body" makes hard power strategies less than successful. Although there have been attempts by the state to physically confiscate or otherwise shut down Internet sites, such as the infamous Operation Sundevil of May 1990 where the American Secret Service seized 42 computers in a nation-wide sting against illegal activities online (Sterling 1992: n.pag.), such campaigns have ultimately proven ineffective due to the acephalous nature of the medium. An Internet server shut down in the American Midwest may reappear in Norway or Rio, beyond the reach of American law enforcement. Likewise, due to the exponential proliferation of World Wide Web sites in the past few years, just keeping track of what materials are made available, and where, is a daunting task.

1.6 Conclusion

The rizomatic, fluid nature of the matrix offers what may be described as a functioning, global anarchist medium largely free from any central power or governing agency and molded according to the desires and convictions of its constituents. Through this chapter, we oversaw the principal theoretical elements involved in information

warfare, and more specifically the Zapatista netwar. Our discussion of the nature of information helped set a basis from which to discuss the use of information and its relationship to knowledge and action. This led us to a section on hierarchy and the contrasting notions of control and coordination, which constitute a vital concept in our understanding of information warfare. Because one of the most powerful online strategies involves soft power and coordination rather than hard approaches involving control issues, a discussion of these two differing approaches work to build a theoretical foundation upon which to base the study. Further discussions involving hierarchy vs. networks further reinforced the rizomatic nature of information warfare, a system based largely on anarchistic principals. Lastly, the point is made that although the matrix is anarchistic in nature, it is not part of an anarchistic political movement. Arising out of people's use of the medium as well as its original purpose as determined by the US-funded Advanced Research Projects Agency (ARPA), anarchism online is the result of its social and physical structure which encourages freedom of expression and makes control a complicated to impossible task. It is these factors which make information warfare online such a new concept, requiring innovative responses on the part of both the state and the wired activist community.

In the next chapter, we will explore the birth of cyberspace as part of ARPA, and reveal how the seeds of cyberculture were sown and grew beyond the realm of state control to include the cyberpunk and hacktivist movements of the eighties and nineties. Through this historical analysis, an understanding of the geography and history of the digital battlefield will be gained and then applied to the Zapatista netwar. This discussion will set the stage for the case study, providing an understanding of the social, cultural and technological factors involved in the rise of information warfare.

Chapter 2
From ARPA to the World Wide Web

2.1 Introduction

In the 1960s, the United States government was very concerned with the threat of nuclear war, and much of its research in both military and scientific realms was committed to topics related to waging and surviving a nuclear exchange (Sterling 1993: n.pag.). Of great concern was the problem of communication, for it was feared that the various governmental and military installations throughout the country would be isolated from major control-and-command centers following a nuclear exchange. This communications breakdown could effectively paralyze the nation, making any kind of organized, effective response highly problematic, if not impossible. Following the belief that in order to understand the present, one must know the past, this chapter presents the early days of cyberspace at the hands of young, idealistic programmers in the employ of the US Department of Defense. Following the growth of computer mediated communication (CMC), the rise of email, newsgroups and chat will be described, along with an overview of the rise of cyber culture and its role in the transformation of CMC from an exclusive government project to a public, largely uncontrolled realm. Through this analysis of the many facets of network communication, the different types of communication options available to the netwarrior will be assessed and the advantages and disadvantages of each noted. The importance of establishing how communication occurs online is basic to an analysis of information warfare, for it reveals the flexibility of the system and the ways in which different communications protocols can be used to best advantage.

2.2 Cyberspace: First Steps

The launching of the Soviet Sputnik in 1957 was a catalyst for American research into computer technology. Already in 1963 Douglas Engelbart, an American scientist and

technological visionary, was funded by the US government to maximize the flexibility and user-friendliness of existing computer systems. As interest in computer-mediated communications grew throughout the 1960's and 1970's, the U.S. Department of Defense created the Advanced Research Projects Agency (ARPA). The goal of ARPA was to push computer systems technology further than it had ever been before, and, if necessary, bypass the standard scientific research "process of peer-review proposals" (Rheingold 1993: 66).

J.C.R. Licklider and Robert Taylor, research directors at ARPA, were involved in much of the original research which was to lead to what is referred to today as cyperspace, and although CMC was still in its infancy, the dream of interactive network communication was already a shared vision.

> 'What will on-line[sic] interactive communities be like?' Licklider and Taylor wrote in 1968. 'In most fields they will consist of geographically separated members, sometimes grouped in small clusters and sometimes working individually. They will be communities not of common location, but of common interest...' (Rheingold 1993: 24)

As the ARPAnet grew, it soon became a nation-wide computer network with links to major research centers across the continental United States (Sterling 1993: n.pag.). Unlike traditional hierarchical structures, this network had no central authority or headquarters, for any such edifice would become an obvious target for Soviet missiles. In order for this new communications grid to work as a "bomb-proof" alternative to existing structures, Bruce Sterling writes in an online article entitled *Internet*, it should follow an horizontal, non-hierarchical structure where all nodes would be equal in status to the other (1993: n. pag.).

Efforts at establishing networks of communication went beyond ARPAnet, however, as students, academics and researchers, originally excluded from the ARPA subnet, saw the great advantages offered by this new technology. In 1969, programmers at Bell Labs designed the UNIX operating system (Nemeth, et al. 1995: 1). Known commonly

as V6, this version of Unix was released free to universities, factor which greatly assisted the spread of the network. As Thomas and Farrow describe,

> [Unix] was to be designed with flexibility and interactive use in mind. Along with interactive use, the architects wanted to make this system secure, yet still facilitate file and information sharing (1989:3)

In 1972, V7, the next version of the software, was released and became the first operating system to be widely distributed, again primarily to universities and research centers (Nemeth, et al. 1995: 1). Because the source code was made available to those purchasing the software, the original operating system could then be modified to suit the owner's individual needs. As more computers were equipped with UNIX systems and linked together in an ever-growing subnet, a parallel network began to grow alongside ARPAnet (Rochlin 1997). This opened new areas of opportunity for the creation of far ranging communication networks, and in the process loosened the government's control over computer-mediated communication (CMC).

As UNIX quickly spread to desktop computers in colleges and labs across the United States and Canada, programmers across the continent made the transition from passive recipients to active developers. Looking back at the roots of the matrix, one immediately sees strong counter-culture elements which pointed the way for the hackers, phreakers, cyberpunks and hacktivists who would later take to the cyberspace in the name of freedom, justice, creativity, or just the thrill of breaking all the rules.

As Nigel Clark observes,

> At the height of the 1960s counterculture... electronic technology and an immaculate nature were frequently imbricated in a single vision. The first microcomputers were developed in the small workshops of counterculturally-minded computer 'hackers' who had gathered in California in the mid-70s and were intended to facilitate self-reliance at a grassroots level: 'The destiny of the microcomputer was to create a global culture of electronic villages cradled in a healthy natural environment- the sort one found scattered through the pages of the *Whole Earth Catalog.*' (1996: 92).

From its birth at the hands of rebellious young programmers, the matrix began to grow into a realm in and of itself, a 'virtual reality' later described by author William Gibson as a

> consensual hallucination experienced daily by billions of legitimate operators, every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. (1984: 51)

According to Clark, the main factors which transformed the matrix from a straightforward means of communication into a virtual space where one could "live", in effect, was the feeling of travel one gets from surfing from one computer system to the next across digital networks and the development of graphical interfaces such as those used in Macintosh, Ms Windows and Unix's xwindows interfaces (1996: 93). This combination of intuitive, graphical interfaces and a huge, steadily growing online population combined to create a virtual world based upon theoretical structures very different from the military and governmental structures that originally financed its creation.

2.3 Usenet

In 1979, at Duke University, a group of graduate students developed the first version of Usenet News, which was to become a major communications protocol (Rheingold 1993).

> Usenet, meant to represent Unix Users Network, was designed as a forum for discussion about Unix and for Unix troubleshooting. Unix itself was deliberately designed to foster a professional community of programmers who used Unix toolbox to create new tools that all other Unix toolbuilders could use... [The inventors of Usenet] were surprised at how hungry people were for all kinds of conversations on a worldwide basis, once they caught on to this strange new idea of a conversation in text that floated from campus to campus around the globe. (Rheingold 1993: 117)

Although Usenet works along similar lines in that messages are sent as ASCII text, the address is not an individual or a series of individuals but a topic of discussion, known as a newsgroup. Should someone wish to respond to a posting, he may either post a reply to Usenet or send the author of the message personal email (Rheingold 1993). In this way, email and Usenet combined to form a distributed system both public and private.

The structure of Usenet is composed of main subject headings under which subheadings are listed, followed by additional subheadings all the way down the tree. Because of the low cost of entry into Usenet, and the fact that most universities offer it free to students and faculty, the popularity of this international conferencing system has increased rapidly (Shade 1996: 12). When Usenet News was first introduced in 1979, there were three Usenet sites distributing an average of two articles per day (Rheingold 1993: 119). In 1980, the number of hosts running Usenet increased to 15, with a circulation of 10 articles per day. In 1981 there were 150 sites and in 1987 the numbers grew to 5,000 with a circulation of about 20 articles per day (Rheingold 1993: 120). Leslie Regan Shade, in an essay entitled "Is There Free Speech on the Net? Censorship in the Global Information Infrastructure", describes the level of popularity to which Usenet had risen by the early nineties;

> ...in a two-week period in May 1992 there were an estimated 240,000 articles posted, totaling over 445 million bytes, submitted by over 20,000 different users to 4,500 newsgroups for an average of 32 million bytes per day. There are further estimated to be 2 million people at 40,000 sites in the US, Canada, Europe, Japan, Korea and Australia who read news. (Greenberg and Hall, qtd. in Shade 1996: 13).

Once the realm of government-funded researchers, the Internet was now home to thousands of students interacting with each other through newsgroups and electronic mailing lists. By 1989, there were an estimated 120 thousand computers connected to the Internet, and by 1992 the number had climbed to 740 thousand with over a million

users (Rochlin 1997: 44).

2.4 Bulletin Board Systems

As Usenet was gathering momentum as a means of popular communication, another type of CMC was rapidly gaining popularity among the young and information-hungry pioneers of the digital age (Rheingold 1993). Bulletin Board Systems (BBSs), like Usenet, enabled adherents to exchange text messages as well as audio and graphic files. All that was needed to run an effective BBS was a personal computer, BBS software which could usually be obtained from either Usenet or other BBSs, a modem and access to a telephone line. Much of the BBS software is also quite configurable, enabling system operators (sysops) the freedom to tailor the "look-and-feel" of their digital kingdom according to their own desires and ambitions.

Unlike ARPAnet, which was first controlled by government and then by private enterprise, BBS culture was free and open, power being now re-distributed amongst a wide body of system administrators, or sysops. Although each individual sysop retained ultimate control over his or her BBS, the vast numbers of BBSs meant that users could avoid unfriendly boards by frequenting BBSs more attuned to their needs. The result was the creation of a BBS counter-culture, where, as Rheingold describes,

> ...an ordinary person anywhere in the world [can become] a publisher, an eyewitness reporter, an advocate, an organizer, a student or teacher, and potential participant in a worldwide citizen-to-citizen conversation. The technology of personal telecommunications and the rich, diverse BBS culture that is growing on every continent were created by citizens, not doomsday weapon designers or corporate researchers. (1993: 131)

2.5 Chat

Chat, the medium ruling much of the BBSs, is different from either Usenet or email in that communication occurs in "real-time" as opposed to postings or messages which can be stored, and replied to, at a later date. Like email, chat was born with the invention of *time-sharing* as part of the Unix systems back in the early days of ARPAnet (Rheingold

1993: 178). Using a program called "talk," a Unix user could connect to another Unix user anywhere in the world and carry on a conversation as one would using a telephone, the difference being of course that while the phone was verbal in nature, chatting was a purely text-based CMC medium.

In 1988, a programmer at the University of Oulu, Finland, wrote the first Inter-Relay Chat (IRC) program, a "multi-user synchronous communications tool designed to function across the Internet" (Rheingold 1993: 179). The coming of IRC revolutionized Internet chat, for it allowed multiple users to communicate at the same time ("synchronous") in real-time, as opposed to email which occurred over a more extended period of time. Moreover, IRC servers did not usually record chatting sessions, making the medium ephemeral, for words once typed quickly disappeared to be replaced by the typed words of others. Due to chat's synchronous nature, it was common to have several conversations happening simultaneously between different people in a single channel, with seemingly unrelated words scrolling down the screen.

The three fundamental elements of chat culture are 1) synthetic but stable identities, 2) quick wit and 3) the ability to convey and maintain an emotional context through the exclusive use of text. This is done largely through the use of *emoticons*, textual constructs such :-), to indicate happiness, :-(, to show unhappiness, or :-0 , which means the user is screaming. Because of the anonymity conferred through IRC, a deep level of intimacy is often reached between participants, resulting in the sharing of real-life secrets that were seldom (if ever) discussed in real-life. These intimacies breed an apparent contradiction in that although it is expected for participants to assume a fictitious persona, loyalty and honesty within the parameters of this fictitious identity is of paramount importance.

Like Usenet, IRC is divided into quasi-unlimited numbers of channels, each one dedicated to a specific topic. During the Persian Gulf War, IRC took on an important role

as people from around the world gathered in select IRC channels to discuss, share information and offer support. Internet access had been established from Kuwait before the Iraqi invasion, and continued for a week after all radio and television broadcasts had ceased. Iraqi students used this medium to provide eye-witness accounts to an international audience which then redirected their messages to newsgroups, web sites as well as traditional media.

What follows is an excerpt from the Peace IRC Channel during the beginnings of the war,

> IRC Log started Thu Jan 17 19:43
> *<EricBlade> Sorry about this, need to test a new client function to make sure I can send to this channel.*
> *-> *banshee* thank you*
> *-> *ericblade* it came through.*
> **EricBlade* Thanks.*
> *<Python:+report> palestinia sources say 5 explosions... 1st one 2:20 israel time (cnn)*
> *-> *nati* Hi, I am chris.... I am sorry to hear about this ... I pray for you and your family*
> *<Enigma:+report> saudi arabian f-15 missed*
> *> nbc says major attack*
> *<cos> Israel says one chemical warhead hit Tel Aviv*
> *<bunny:+report> there is also a thunder storm accompanying the missile attack*
> *> from pentagon says israel has "jerico" [sp] to respond immediately.*
> *<Ryman:+report> NBC: Pentagon says its a major attack*
> **Swan* scott@!! this is swan could you make me a moderator?*
> *<Mustang:+report> is anyone watching cnn?*
> **cos* "Jericho"*
> *> victims of chemical warfare have been taken to hostpital*
> *> I dont have cnn*
> *<Mustang:+report> scot: so it was chemical then?*
> **Swan* scott! helpppp meeee*
> *<bunny:+report> i have CNN on right now*
> *<EricBlade> Is Nati gone?*
> *<Swan> test*
> *<Python:+report> cnn is trying to talk to security chief at sheraton in tel aviv (unsuccesfully)*
> *<Python:+report> nati is still on, but not saying anything*
> *> nbc says pentagon has verified 1 chemical missile has hit tel aviv*
> ➢ *tom B. is speachless [sic].* (Gulf War IRC Logs 1992)

This exchange continued as war raged across the country, providing a vital

communications link when most others were down. Furthermore, the unregulated nature of chat made possible a direct interaction between people whom otherwise could not have communicated. As Reid states, "I am told that users from the two countries [U.S. & Kuwait] often interacted [over IRC] with very few disagreements and mostly with sympathy for each other's position and outlook" (quoted in Rheingold 1993: 185).

2.6 Electronic Mail

Electronic mail (email) has always been one of the most important aspects of computer-mediated communication (Rheingold 1993: 72). Like chat, email necessitates only the most minimal system set-up, making it an ideal media for most relatively poor non-governmental organizations as well as individuals not connected to either universities or state-approved research labs (Bennahum 1998). One of the main advantages offered by email is the capacity to create a mailing list, which can reach any number of people instantly. What makes mailing lists so powerful are the number, and the identity, of its subscribers. As Bennahum states,

> What is exchanged on a list, where money rarely is the prime measure of success or failure? Ideas, time, and attention- the sometimes vast numbers of subscribers, or powerful people on the list- are all part of a complex ecology in an environment remarkably separate from traditional markets, where getting something for nothing remains a paradox... It's a place where traditional models lose their meaning and power comes not from wealth, but from thought. (1998: n. pag.)

Unlike other media such as newspapers and television, mailing lists required the active participation of some of its members in order to survive (Bennahum 1998). Although there are always more "lurkers" than active participants on any given list, the option exists for all who wish to participate to do so. Likewise, unlike traditional media which requires considerable financial resources to produce, email is financially accessible. Although the necessity to own a computer, modem and telephone line could be seen as a financial barrier, non-profit organizations such as Free-Nets go far in making the technology available to the general public. Combined with public-access

computers such as those found in many municipal libraries, Free-Nets bring the matrix to the people by undermining the financial barrier and ensuring popular access.

> Because it's so ubiquitous, list publishing is powerful: reaching one person is as easy as reaching a million. Since most lists are free, the barrier to receiving them is very low. All you need is an email account. List publishing is the devolution of mass media into the hands of everyday people- people who can, with almost no overhead, gestate and spawn enormous publishing empires of their own, or, if they choose, small intimate salons, private salons, private spaces between friends. Whatever the scale- from the nearly 1 million-person list (CNET's *Digital Dispatch*, one of the largest lists in the world) to the two-person list, the cost of production and distribution is extremely low. (Bennahum 1998)

As of 1998, it was estimated that between 150,000 and 350,000 mailing lists were in existence, with an increase of 5 to10 percent per month (Bennahum 1998). The discussion subjects are incredibly varied, from soap opera discussions and Hollywood gossip to writer's workshops and scholarly discourse. Most of these lists rely on word-of-mouth to grow and prosper, and as there are few copyright issues to deal with, information released on such lists can potentially reach a very large audience, very quickly.

2.7 The World Wide Web

In the early 1990s, researchers at the European Laboratory for Particle Physics (CERN) and the World Wide Web Consortium (W3C) developed the World Wide Web (W3), a graphical navigation protocol based on hypertext technology (Cailliau 1995: n. pag.). Hypertext is "a method of presenting information where selected words in the text can be 'expanded' at any time to provide other information about the word. That is, these words are *links* to other documents which may be text, files, pictures..." (Krol 1992: 228). Embedded within each link is the Uniform Resource Locator, or URL, which holds the address of the document to the target document. Because of the capacity of W3 to communicate with different protocols, the target of the URL can be a text document, audio or video file, Usenet post, FTP or Gopher menu (Berners-Lee & Cailliau 1992: n.

pag.). This flexibility allowing for the use of previous navigational technologies and the ready access to Usenet and email made the Web all encompassing in a way unmatched by any previous technology. Even multi-user dungeons (MUDs) and chat, considered by many as one of the best examples of virtual communities, can be accessed through the Web.

2.8 Conclusion

Through this exploration of the birth of CMC, an historical framework has been erected within which to conduct our study of information warfare. We have followed the growth of cyberspace from a secret military project to an unregulated, global communications medium encompassing millions of users, with hundreds more coming online every day. By investigating the different communications protocols used in cyberspace, we have seen how CMC is carried out and the manner in which information can be shared across the networks. The characteristics of chat, email, Usenet and the Web have been accessed, thus providing a basis upon which to explore the development of the Zapatista netwar. By understanding the tools, or, dare I say, the weapons of information warfare, we can better appreciate the factors contributing to the effectiveness of Digital Zapatismo. In the next chapter, we will take a more political approach to the matrix as the theme of information warfare is introduced. Following works by academics, military analysts as well as online activists themselves, a portrait of the digital battlefield will be drawn. The chapter will close with an overview of some of the most prominent wired activists today, and their impacts upon the political and social fabric of the international scene.

Chapter 3

The Rise of Netwar

3.1 Introduction

As computer-mediated communication (CMC) increased in popularity and more people established themselves in cyberspace, political activists began to recognize the potential of the matrix as an alternative field for aggressive action. Using soft power as their initial strategy, online activists, or "netwarriors," wasted little time in adopting the network form and exploiting the acephalous nature of cyberspace to their own advantage. Growing from this crucible of rebellion came the netwarriors, who with speed and adaptability challenged traditional institutions and threatened to undermine their foes through informational superiority. Using material from military analysis, political speeches, as well as the words of contemporary netwarriors and hacktivists, an overview will be provided of information warfare and its practitioners. The Association for Progressive Communication, one of the largest online activist organizations will be featured and its impact upon the world stage assessed, as well as the impact of the Yugoslavian Radio B92 during the NATO War in Kosovo. In the section on hacktivism, the methods employed by radical info-warriors will be seen and their exploits placed within a political context. A discussion will also be offered on the effectiveness of aggressive online tactics, closing this enquiry into the nature of netwar.

3.2 Netwar

John Arquilla and David Ronfelt, both analysts with RAND Corporation, have explored the contrast between traditional hierarchical structures, such as corporations and governments, and the cyberspatial networks employed by wired activists. Through the use of soft power, wired activists are perceived as constituting an informational threat to hierarchical structures, for in cyberspace conventional definitions of power, that

is, power based on physical force and direct authority, are often supplanted by psychological manipulation and subtle (dis)information campaigns.

In order to identify and categorize this new threat to the political and economic *status quo*, the authors describe network-based activism as either netwar or cyberwar (1997). Unlike cyberwar, which defines the aggressive and/or battlefield use of computer technology, netwar involves the use of soft power in information-oriented conflicts most likely to involve small, semi-independent actors acting in concert.

> [Netwar is a] mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use- indeed, depend on using, network forms of organization, doctrine, strategy, and communication. These protagonists generally consist of dispersed, often small groups who agree to communicate, and act in an internetted manner, often without a precise central leadership or headquarters. Decisionmaking may be deliberately decentralized and dispersed. (1997: 277)

Following the original strategy espoused by the Department of Defense (DoD) during the Advanced Research Projects Agency (ARPA) project, the new "info-warriors" adopt speed and flexibility as their main tactics. Through a structural design both "acephalous" (headless) and "polyphalous" (hydra-headed), networked activists negate the possibility of a "quick kill" by which opponents can disable a campaign by striking at the leaders. Thus enveloped in a "digital cloak," netwarriors can rapidly spread information and undermine the credibility of their opponent while avoiding discovery and possible termination by the state. Because of their speed and skill in navigating digital space, netwarriors in conflict with traditional hierarchical structures generally force their opponents to adopt a defensive posture, forcing them to react to their actions rather than initiating their own informational strikes.

The lack of central leadership, however, means that in order to succeed netwarriors require a high degree of dedication and ideological cohesion or a powerful common vision. Indeed, one could say that it is this vision, this cause, which assumes the

leadership role and sparks the flame of action in the hearts of those who hold it dear. As RAND observes, in order to succeed netwarriors must subscribe to

> ... a powerful doctrine or ideology, or at least a strong set of common interests and objectives, that span all nodes, and to which the members subscribe in a deep way. Such a doctrine can enable them to be "all of one mind" even if they are dispersed and devoted to different tasks. It can provide an ideational, strategic, and operational centrality that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that they do not have to resort to a hierarchy- "they know what they have to do." (Arquilla & Ronfelt 1997: 280)

There are three major types of grassroots organizations active in online activism: activists, infrastructure-building and network facilitating organizations. While activists are largely composed of individuals with, among others, indigenous, human rights or environmental sympathies, infrastructure-building organizations such as the Association for Progressive Communication (APC) specialize in building internet connections and shaping networks across which information can be spread quickly and efficiently (Ronfelt & Martinez 1997).

Established in 1989, the APC has since become a "consortium" of over 25 independent networks involving over 50,000 activists in 133 countries (APC 1989). While not fighting for any specific cause, the APC provides the expertise and the technology many NGOs require in order to effectively coordinate actions such as letter/fax/email campaigns, public demonstrations and caravans. Also, the APC assists grassroots organizations in developing networks of solidarity with others across the country or across the world, and this at a much lower cost than would be incurred through commercial Internet providers.

For example, in Africa the Maasai people of Tanzania were losing their land to commercial farming enterprises, development projects, mining and conservation interests. Poor and generally illiterate, the Maasai were poorly equipped to fight the developers and capitalists intent on developing their homeland. Through the APC,

however, an NGO called EcoNews Africa used the matrix to bring to the attention of many outside the country the plight of the Maasai, thereby enabling them to voice their concerns over their lack of control over their land as well as their fears for the future to a much wider audience. Although the issue is not yet resolved, what could otherwise have been an isolated tragedy of poverty and stolen lands has become a public issue before the global community. Commenting on EcoNews Africa's campaign, the Maasai "expressed that they were happy to be part of a larger global community that was watching, concerned and taking action" (APC 1989: n. pag.).

According to information posted on their web site (www.apc.org), the Association for Progressive Communication was also successful in bringing justice to jailed Russian activists, assisting landless peasants in Brazil as well as providing communications networks for peace workers in the former Yugoslavia. On a web page entitled "About the APC," part of the greater APC web site, the organization outlines the services provided to activist organizations around the world. These include,

- Internet Access
- Training and Support: For Users, Trainers and Facilitators
- Exclusive News and Information Services
- Communications Consulting
- Online Collaboration Strategies and Methodologies
- WWW Site Development
- Public and Private Workspaces: Mailing Lists and Newsgroups
- Customised Information Tools: Databases and Search Engines (APC 1989: n. pag.)

By offering such services, the APC undermines potential financial and technical barriers by providing not only access to the matrix but also training in the technical and strategic fields required to make optimal use of the network form of communication. By training activists in the art of networked information warfare, the APC undermines state and corporate informational hegemony, in effect enabling civil actors to use the state's

own weapons against them. By making technology accessible to those who otherwise would not have access, the APC has

> broken governments' monopoly on the collection and management of large amounts of information and deprived governments' of the deference they enjoyed because of it. In every sphere of activity, instantaneous access to information and the ability to put it to use multiplies the number who command great authority. (Mathews 1997: 51)

On September 9-11, 1998, the APC took part in the *International Forum: Communication and Citizenship* which took place in San Salvador, El Salvador (ALI 1998). Hosted by the Agencia Latinoamericana de Informacion, the role of the Forum was to serve "as a meeting point [for] a variety of social groupings, so that they [could] draw up proposals and actions in favor of [achieving respect for human rights], reinforce each others' initiatives and that movements for the pro-democratization of communication might converge" (IFCC 1999: n. pag.). Like Barber (1995), Sardar (1996) and Schiller (1995), the APC realizes the threat posed by the corporate media, describing how these

> ... have strengthened their traditional status as a power factor, to the point where they have assumed a role of social control, previously fulfilled by other institutions. It is now commonplace that the media determine what is socially relevant or not, who is worthy of being considered a social actor, etc., thus seriously distorting democratic processes. If citizens do not take on this issue, the danger of "media or computerized fascism" threatens to become reality. (IFCC 1999: n. pag.)

In the opening round of the NATO war in March, 1999, a group of Belgrade university students turned to the Internet when the Milosevic government shut down their independent radio station Radio B92 (Mandelbrot 1999: 29). Founded in 1989, Radio B92 had become a focus for those opposed to the Milosevic government and the wars in Croatia and Bosnia, acting as a center for alternative media and activist organization. Forced to look for alternative methods of broadcasting following the shutdown of the station, the Yugoslavian journalists took to cyberspace by erecting a web site where they broadcasted news, eyewitness accounts and provided a forum for discussion. "We use

the Net for coverage of Kosovo," said Sasa Mirkovic of Radio B92 at the Freedom Forum conference. "The government closed down transmitters but could not close down Net access" (Docherty 1999: n. pag.).

On May 15th, 1999, Radio B92 broadcasted NetAid, a 24-hour mix of music and messages of peace. The goal of the broadcast was to draw attention to censorship of the media in the Balkans and, like the Zapatista situation described below, appeal to the world community in working for peace in their homeland. Musicians participating in the broadcast came from around the world, including US band Sonic Youth, Latvian media-art group E-Lab and Canadian artist John Acquaviva. Among the many messages of support sent to NetAid was one from fellow journalists that read, "Dear friends! We are Minsk Radio 101.2, closed by Lukashenko three years ago.... Your experience of fighting and working is a good example for us and everyone who respects freedom of speech and liberty" (Martz 1999).

The rise of international webs of communication can be seen in the actions of indigenous networks of support for the revolutionary cause of the Mexican Exersijio Zapatista de Liberatión National (EZLN). Imprisoned American Indian Movement (AIM) leader Leonard Peltier, for example, wrote in a letter to the EZLN, "[y]our struggle, which was so magnificently brought to world attention on January 1st is an inspiration to all of us. Your blood is our blood. Your fight is our fight. Your victory is our victory" (Peltier 1995: 140).

Furthermore, on January 9, 1998, an article appeared in *Mohawk Nation News* denouncing the Kahnawake Band Council for taking part in the signing of the North American Free Trade Agreement (NAFTA) with the people of the province Oaxaca, which borders with Chiapas.

> There's been intense opposition by the Mohawk people in Kahnawake Mohawk Territory against [Chief Joe] Norton and Delisle and their business proposition and their theft of Iroquois cultural symbols in

> collaboration with Canada and Mexico. The deal between Canada and Mexico is to set up labour camps in Oaxaca to make Iroquois arts and crafts for worldwide marketing ... There is a lack of permission and support for 'Project OK' because it is illegal according to Iroquois law and the UNESCO convention on intellectual and cultural property passed in 1970. But mostly because it violates the human rights of Indigenous People in Mexico who have rebelled against NAFTA. Canada, Norton and Delisle will be exploiting cheap Indigenous labour in Mexico, which the Indigenous people are resisting. This resistance has lead to tragic consequences such as the recent massacre in Acteal. The Mohawk are angered and disturbed by their determination to go to Mexico with the Canadian government to sign this deal under NAFTA. (MNN 1998: n. pag.)

NAFTA came into being in 1992 and involves Canada, the United States and Mexico. Under this agreement, many of the restrictions on cross-border investment and other transactions are lifted, creating the largest free-trade zone in the world including over 360 million people and an economic output of $7 trillion (Guy 1998: 389). The restructuring of the countries' economies in preparation for NAFTA is of great concern to many, particularly peasants, workers and indigenous peoples who see this process as further erosion of their rights and deepening of the divide between rich and poor. As Noam Chomsky describes,

> NAFTA is expected to drive large numbers of workers off the land, contributing rural misery and a surplus of labor. Manufacturing employment, which declined under reforms, is expected to fall more sharply. A study by Mexico's leading business journal, *El Financiero*, predicted that Mexico would lose almost a quarter of its manufacturing industry and 14 percent of its jobs in the first two years after the enactment of NAFTA... These processes should depress wages still further while increasing profits and social polarization, with predictable effects in the United States and Canada. (Chomsky 1995: 178)

Although not directly supportive of the Zapatista, the Mohawk's opposition to NAFTA bridges the gap between the Mohawk and the indigenous peoples of southeastern Mexico, providing yet another link in the guerillas' web of resistance. The Mohawk recognize this link in their mentioning of the Acteal massacre, recognizing the interconnectivity in Chiapas of both human rights and economic issues.

Environmental groups, described by Cleaver as having developed a "highly elaborated cyberspatial sphere for the sharing of innovative alternatives to current ways of doing things" (1997: n. pag.) have also played a significant role in the Zapatista netwar. Cleaver notes how

> serious attempts to rethink the interconnections between humans and their environment has led to considerable overlap with an array of cultural experiences and philosophies outside the Western traditions from which capitalism emerged. Amidst that array the practices and thinking of a variety of indigenous peoples have received considerable attention and many elements of their diverse approaches have received a surprising degrees [sic] of acceptance" (n. pag.).

This "interconnection between humans and their environment" brought together actors from different spheres of interest, forming unlikely coalitions that bridged traditional divides.

3.3 Hacktivism

Hacktivists, a term first coined by the hacker cell Cult of the Dead Cow (cDc), describes the digital equivalent of radical activists, info-warriors using their talents to conduct direct assaults on the informational infrastructures of political foes, incapacitating and sometimes even crippling web sites and internet servers (Romano 1999). Aggressive, technically-skilled and highly political, hacktivists constitute a "convergence of the computerized activist and the politicized hacker," (Wray 1998: n. pag.). Using time-tested strategies such as civil disobedience and sabotage, hacktivists target the informational infrastructure in an attempt to propagate their beliefs and punish their opponents. Stephen Wray, activist and co-founder of the Electronic Disturbance Theatre (EDT), emphasized in a presentation to Harvard Law School's Berkman Center on Internet and Society how

> [a] common understanding of civil disobedience is predicated on the notion that there are times when it becomes necessary to break a law, or a set of laws, that appear unjust in comparison to what some would call a higher law. In the late 1950s, civil rights activists broke laws in the South that prohibited African Americans from sitting at the lunch counters of

> then white-only establishments, motivated by a higher law or set of moral codes. (Wray 1998: n. pag.)

Continuing, Wray describes how the term "electronic civil disobedience" was originally coined by a group of scholars and artists who, in 1994, published a book entitled "The Electronic Disturbance" and in 1996 released another work titled "Electronic Civil Disobedience and Other Unpopular Ideas." The works, as Wray describes them, offered a

> ... theoretical exploration of how to move protests from the streets onto the Internet. They examine the tactics of street protest, on-the-ground, disruption and disturbance of urban infrastructure, such as building entranceway blockades or takeovers of traffic arteries, and they hypothesize how such practices can be applied to the Internet infrastructure. Underlying our usage of the term "electronic civil disobedience" is a keen interest in continuing this exploration of moving protest tactics from the street to virtual or digital realms. (Wray 1998: n. pag.)

"Blondy" Wong, a Chinese dissident living in Canada, is the leader of a Toronto-based hacker cell known as the Hong Kong Blondes (Paquin 1998: n. pag.). Wong, a survivor of political persecution in his home country, is presently waging a cyberwar against the Chinese government to protest widespread human rights abuses. Although the Chinese government will not confirm the effectiveness of Wong's attacks, the hacker claims to have infiltrated the Chinese military and security networks. In an interview with the cDc, Wong describes the factors involved in the rise of hacktivism.

> There has been a shift in consciousness, I believe. Younger people have a great deal of talent.... I think they are different from the generation of hackers before them. They want the recognition and attention, but they also want to do something to contribute to change things in a positive way. In general, I think what they are doing will grow and turn into something that makes a difference. (Qtd. in Ruffian 1998: n. pag.)

Within the global, unregulated field of the matrix, hacktivists found not only the weapons to express their wrath but also the political and theoretical structures within which to operate. Commenting on the necessary relationship between knowledge and action, Wong says,

> There are many ways to get involved to support the struggle for human rights.... Becoming aware is the beginning. Just talking about it is important, educating yourself. But if we are talking about the hacker community, you know, what they can do, this really is a matter of personal choice. I think that if people want to participate they should use the skills that they have. (Qtd. in Ruffian 1998: n. pag.)

Sharing Blondy Wong's outrage at China's human rights record, hackers Bronc Buster and Zyklon, both members of the loose hacker collective Legions of the Underground, broke into a Chinese government-run website and rewrote the homepage with a rant against the state's dismal record of abuse and oppression (Romano 1999: 170). Impressed with the media coverage garnered by this attack (MSNBC, CNN and Reuters all covered the event), the hackers broke into China's Internet servers and sabotaged the firewalls, security measures aimed at controlling user access to the Internet (Romano 1999: 172). Through the use of firewalls, system administrators can ban individual websites and USENET groups, thereby exercising great control over access to online information. Considering this as another form of oppression by the Chinese state, the hackers proceeded to delete the lists of banned files, thereby granting Chinese Internet users access to sites never before available. "They blocked everything you could imagine," Buster recounted to Spin magazine, describing the censoring effects of the Chinese firewalls. "From news sites and human-rights sites to Web sites like Family.com and Parents.com... For a while, people were allowed free [Internet] access in and out of the country. We had really done something positive" (Qtd. in Romano 1999: 172).

On August 1, 1998, a Portuguese hacktivist cell called Kaotic Team expressed their disapproval of the Indonesian invasion of East Timor by hacking into Indonesian Internet servers and "altering" 45 government web sites (Paquin 1998: n. pag.). The action consisted of writing messages across the web sites calling for an end to the genocide in East Timor and the alleged torture and rape of ethnic Chinese during the anti-Suharto

riots. One message, "cut" into the front page of the Indonesian State Ministry For Population/ National Family Planning Coordinating Board web site, read, "Did you see the disorder in May? And do you want to see another disorder in your internet? We come here JUST to make our protest against your violence. I don't want to make any data-losing in your NET" (Glave 1998: 1).

In a New York Times article, Secretos, a member of Kaotic Team, talks about the cell's agenda and online strategy, "We have hundreds of servers we could hack, and we don't... By contrary [sic], we even help them to fix their bugs. The main objective of our hacking pages is to transmit the message" (Qtd. in Harmon 1998: 5). Canadian foreign affairs minister Lloyd Axworthy emphasized the growing power of CMC in a speech at an NGO conference in September of 1998. He said,

> ...technology is changing the equations of power, challenging the conventional channels of communication, distributing and disseminating influence in the broadest possible fashion, to the point of democratizing the channels and getting rid of the gatekeeper.... The technology has a mind-boggling potential to break through barriers and overcome political obstacles to educate, inform and be an agent of political change... The mouse is mightier than the missile. (Qtd. in Paquin 1998: n. pag.)

On August 25, 1998, in their first bulletin the EDT declared their intention to strike at the Mexican government, the Pentagon and the Frankfurt stock exchange in a bold move in support of the Zapatista.

> In solidarity with the Zapatistas, indigenous peoples in Chiapas, others resisting the Mexican government, the global pro-Zapatista movement, and people everywhere struggling against neoliberalism and the global economy, the Electronic Disturbance Theater urges SWARM actions, multiple acts of Electronic Civil Disobedience, on Wednesday, September 9, 1998....
>
> To demonstrate our capacity for simultaneous global electronic actions and to emphasize the multiple nature of our opponents, FloodNet will target three web sites in Mexico, the United States, and Europe representing three important sectors: government, military, and financial.
>
> In Mexico, FloodNet will target President Zedillo's web site...an obvious choice and one we have made before. In the United States, FloodNet will target the Pentagon, ...also an obvious choice given the level of U.S.

> military and intelligence involvement in Mexico. And in Germany, FloodNet will target the Frankfurt Stock Exchange, a less obvious choice, but one that makes sense as it is a key European financial site with high symbolic value. (Chronology of SWARM 1998)

As Carl Kaplan describes in an article written for The Cyberlaw Journal: New York Times on the Web, FloodNet, a program written in the Java programming language, is relatively easy to use:

> ...a web surfer connects to Flood Net, which appears on the Internet only at an appointed time, so as to avoid detection. Flood Net automatically connects the surfer to a pre-selected Web site, and the software automatically hits the selected site's reload button every seven seconds. If thousands of surfers connect with Flood Net during a particular day, the mass of activists could disrupt the operations of the particular site. (1998: 2)

Unlike Kaotic Team and the Hong Kong Blondes who operate in secrecy and are composed of relatively few members, the EDT relies on mass international support to fulfill its goals. According to Wired magazine, up to 10,000 people took part in the Flood Net attack, generating a total of 600,000 hits to each of the three targeted web sites (McKay 1998b). The Pentagon, however, knew of the attack and launched a defensive strike with its own Java applet, called Hostile Java, which caused multiple copies of the browser to load and reload in the attackers' desktop, eventually causing a systems crash.

Faced with the Pentagon applet, FloodNet retreated and ceased its attacks on the Pentagon web site. Nevertheless, it has since initiated attacks against the School of the Americas, the White House, as well as additional strikes against Zedillo's web site. Not everyone is in agreement with the legitimacy of FloodNet, however, and the EDT has been the target of some harsh criticism.

Shortly following the opening of the September 9 hostilities, Hackers Electronic Art (HEART) issued a harsh critique of the EDT and its use of FloodNet in support of the Zapatista,

> FloodNet is both ineffective due to the upstream cache and pure evil, since it represents an abuse of the network. Even if the load was to take down a server (ignoring the free speech implications for a moment, free speech you want for yourself but deny to those with whom you disagree), you would not only impact communications with the target site, but also to those around it. FloodNet is *unacceptable* network abuse. As bad as spam, if not worse. (Chronology of SWARM 1998: n. pag.)

Roy Bourgeois, founder of the School of the Americas, also voices concern over the legitimacy of FloodNet as an activist strategy, saying "[w]e believe in putting our bodies on the line, not our computers.... We have members serving six to 18 months in prison for protest action" (McKay 1998a: 1). "I see it as somewhere between a digital sit-in and 'cybotage,'" adds Ronfelt of the RAND Corporation. "They are trying to crash Web pages and servers. It's aggressive" (Kaplan 1998: n. pag.).

Both Wray and Dominguez, co-founders of the EDT, agree that the use of Floodnet alone is unlikely to cause the Mexican government to change its policy towards Chiapas and the Zapatista (Kaplan 1998). However, they claim, "the protest tactic is designed to create a form of electronic theater that indirectly increases solidarity among activists and propagates a political message to 'other layers of the Internet'" (Kaplan 1998: 3). X-Ploit, a Mexican hacktivist group, echoes Wray and Dominguez's claim, asserting that "[h]acktivism is a way to be heard by millions...We want to speak out about what we and many, many people disagree with in this treasonous and corrupt government. If we protest off-line, we'll have a better chance to see a change" (Harmon 1998: 3). Thus, rather than acting solely as a means of direct action against an opponent, many hacktivist actions serve as a gathering point for online activists, giving members the hacktivist community at large the opportunity to act together in a common goal and thereby fostering a sense of community.

3.4 Conclusion

By defining the crucial concepts of netwar within a contemporary setting, informational warfare is placed within a structured framework from which future analysis

can now proceed. Following the writings of both RAND analysts and online activists, we explored the shadowy world of netwar and described the impact of networked activists on hierarchical institutions such as corporations and governments. A study of the Association for Progressive Communications demonstrated how global activist organizations can spread both the awareness as well as the technical skills required for online campaigns. This global view of netwar is very important with respect to understanding the Zapatista netwar, for it is this flexible, borderless nature that makes information warfare so powerful. Through its flexible and hydra-headed structure, the matrix evades central control and provides an unlimited field of action for those skilled in its ways.

Against this field of activism and rebellion, we will next see how the state is working to tighten its grip on cyberspace. Through the use of Libertarian theory applied to cyberspace, the chapter will explore how the state is working to extend its influence and control online content. Furthermore, we will see how intelligence agencies worldwide are using the Internet to pursue the covert monitoring of civilian individuals and organizations. Skilled in the arts of surveillance and psychological operations, we will reveal how these agencies have recognized the potential of the matrix as a way of extending their influence and have quietly insinuated themselves into the lives of private individuals the world over.

Chapter 4
The State

4.1 Introduction

This chapter explores the relationship between state censorship and control through Libertarian theory. Through a discussion of Libertarianism and its relationship to US attempts extend its influence over the Internet, an argument is offered for the Clinton administration's campaign to suppress free speech and the importance of maintaining of free speech online. This will be followed by an overview of the role played by intelligence agencies such as the National Security Agency (NSA) and the US Secret Service in monitoring and controlling online actors. Drawing from a variety of sources, we will see how strategies being implemented by both private and governmental agencies threaten to undermine this open, anarchistic environment. Maintaining an awareness of the potential for online censorship or surveillance is important to the study of netwar, and in particular the Zapatista, for it reveals how the matrix may not be as free from potential control as it seems.

4.2 Libertarianism and Censorship

In his discussion of Libertarian theory, Will Kymlicka defines Libertarianism as people's inherent rights to dispose of their property in accordance to their own needs and desires (1990: 96). As he states,

> People have a right to dispose of their goods and services freely ....
> Because people have this right to dispose of their holdings as they see fit, government interference is equivalent to forced labour- a violation, not of efficiency, but of our basic human rights. (Kymlicka 1990: 96)

The definition of goods and services pursued in the Kymlicka essay is based within the market economy, denoting material goods and wealth such as would be taxed by the government. Taking a step from the market economy to the digital fields of cyberspace, the "goods and services" described by Kymlicka may be seen as representing

information and its use by individuals and organizations online. Placed within the informational sphere, Libertarian theory offers an efficient paradigm within which to explore the vital importance of unrestricted freedom of expression in cyberspace.

Following this theoretical approach, it becomes the basic right of people online to possess, post, distribute, and share information, and by extension to discuss this information in whatever manner they choose. Kymlicka defines the right to free exchange of goods/information through three major principles, which are as follows:

1) a principle of transfer- whatever is justly acquired can be freely transferred;
2) a principle of just initial acquisition-an account of how people come initially to own the things which can be transferred in accordance with (1);
3) a principle of rectification of injustice- how to deal with holdings if they were unjustly acquired or transferred. (Kymlicka 1990: 97)

With respect to the informational sphere, these principles of transfer could apply to, for example, a website. Information legally acquired (i.e. shareware, unclassified military information, eye-witness accounts) could be freely posted, distributed through mailing lists or posted to USENET without government interference. A website in support of the Zapatista, for example, should be free to post indigenous eye-witness accounts, Zapatista communiqués and legally-obtained photographs and sound bites to the site whether or not the state agrees with the rebels' politics. As long as the information is justly acquired and does not break the laws of the land, the formula to follow becomes "from each as they choose, to each as they are chosen" (Nozick 1974: 160).

An excellent example of the extent to which the American government is willing to go to censor the Internet is the Communications Decency Act (CDA), a bill proposed by US Senator James Exon in 1985. A clear violation of Libertarian principles, the CDA would have made criminal the transfer over fax, email, html or any other digital medium any material deemed "unsuitable" for children, with sentences including fines up to $100,000 US as well as jail sentences. The far-reaching nature of its vague and subjective

terminology would have given the state authority to extend its power over the Internet and censor any material deemed "obscene" whether or not it broke existing criminal laws.

In his work *Anarchy, State and Utopia*, Nozick describes the role of the state as being strictly limited to "the narrow functions of protection against force, theft, fraud, enforcement of contracts, and so on ... any more extensive state [powers] will violate persons' rights not to be forced to do certain things..." (1974: 160). That the power potentially conferred by the CDA could extend into the political sphere became a great concern for many netizens, and sparked a powerful movement to stop the Act before it became law.

The campaign against the CDA was a success, and although the Act was signed into law on February 8, 1996, it was overturned four months later by a panel of three federal judges who described it as "unconstitutional on its face" and "profoundly repugnant." (Quittner 1996: n. pag.)

> The court went further than the most ardent civil libertarians had dreamed. In a striking 175-page memorandum that was published online within minutes of being handed down, the judges declared the Internet a medium of historic importance, a profoundly democratic channel for communication that should be nurtured, not stifled. Because the Net is still in its infancy, the judges said, it deserved at least as much constitutional safekeeping as books and newspapers, if not more. "As the most participatory form of mass speech yet developed," wrote Judge Stewart Dalzell in an eloquently crafted opinion, "the Internet deserves the highest protection from governmental intrusion." (Quittner 1996: n. pag.)

Writing on the potential impact of such bills as the CDA and its successor, the Child Online Protection Act (COPA), James Harrington contrasts the matrix, a "marketplace of ideas," with the Clinton Administration's vision of censorship and control. This perspective of the Internet as a bustling bazaar of information free from state regulation echoes Kymlicka's Libertarian vision of a free market operating according to the wants and desires of its participants. As Harrington describes,

> we ought to exult in the explosion of Internet's unrestrained expression; the passionate desire to convey ideas and expand creativity is a hundred times better than commercial media's suffocating programs, milquetoast news or boring sound bytes. Mr. Exon's misguided proposal would send a message to Internet users around the world that the United States is more interested in becoming a cybercop than fostering a global marketplace of ideas where all can speak without fear and in the hope of bettering the human condition. (1996: 159)

The affirmation of Libertarian ideals by the Supreme Court emphasized the importance of maintaining free information exchange within the parameters outlined by Kymlicka (1990: 97). It revealed how the US administration is attempting to extend its control over the Internet despite the risks that such a move might stifle the very vibrancy and chaotic energy that make cyberspace "the most participatory form of mass speech yet developed." As these attempts by the Clinton administration have shown, online activists must remain alert to governmental efforts at censorship. Although the CDA was struck down, activists must assume that the battle to maintain a free digital marketplace of ideas is an ongoing one and if the medium is to remain and blossom as a political forum, then a vigilant eye must be maintained.

4.3 Online Security

As the following quote suggests, fear that invisible malefactors could seriously disrupt national communications has been around for over 200 years. In nineteenth century France, for example, long-distance communication initially consisted of a state-owned series of high towers on hill tops sporting large, windmill-like arms. As the electric telegraph threatened to replace the towers as France's prime method of national communication, a French academic wrote,

> No, the electric telegraph is not a sound invention. It will always be at the mercy of the slightest disruption, wild youths, drunkards, bums... The electric telegraph meets those destructive elements with only a few meters of wire over which supervision is impossible. A single man could, without being seen, cut the telegraph wires leading to Paris, and in twenty-four hours cut in ten different places the wires of the same line, without being arrested. The visual telegraph, on the contrary, has its towers, its high walls, its gates well-guarded from inside by strong armed

> men. Yes, I declare, substitution of the electric telegraph for the visual one is a dreadful measure, a truly idiotic act. (Qtd. in Sterling 1993: n. pag.)

Despite these fears, the telegraph did become the default mode of communication, to be later replaced by the telephone and the fax machine as well as computer-mediated communication (CMC) such as email, chat and Usenet. The fear he expressed, however, remains and has fueled much of the efforts on the part of both state and corporate actors to protect themselves against potential digital terrorism or "cybotage." As Rand analysts stated in their evaluation of security in cyberspace,

> With more and more of the activities of individuals, organizations, and nations being conducted in cyberspace, the security of those activities is an emerging challenge for society. The medium has thus created new potentials for criminal or hostile actions, "bad actors" in cyberspace carrying out these hostile actions, and threats to societal interests as a result of these hostile actions. (Hundley & Anderson 1997: 231)

The analysts go on to describe such "hostile actions" as including interruptions in communication, altering or corrupting data, manipulating online systems performance and denying access to vital systems. Although some examples of actual digital attacks, such as a virus attack on an AIDS lab and the widespread theft of calling card numbers from 1992 to 1994, are listed as proof that a threat exists from Cyberia, the report concentrates primarily with the *potential* of online attacks. What *could* happen is the heart of the argument, rather than what has actually transpired.

This "hackerphobia" was well illustrated by events following the AT&T systems crash as a result of software failure on January 15, 1990 (Sterling1994). The crash was huge, interrupting over half of AT&T's phone service and throwing many people in both the public and private spheres into a panic. Despite the fact that the crash was the result of a software glitch, and not of malicious origin, a rumor quickly circulated that the crash was the work of hackers bent on destroying the American communications grid. As Sterling describes,

> The police and telco security...had informants in the computer underground and years of experience in dealing with high-tech rascality that seemed to grow ever more sophisticated. For years they had been expecting a direct and savage attack against the American national telephone system. And with the Crash of January 15 -- the first month of a new, high-tech decade -- their predictions, fears, and suspicions seemed at last to have entered the real world. A world where the telephone system had not merely crashed, but, quite likely, *been* crashed -- by "hackers." (Sterling 1994: n. pag.)

In the world of cyberspace security, according to the RAND Corporation, no distinction can be drawn between crime and warfare (Hundley & Anderson 1997: 232). Of serious concern to the US military is the widespread reliance of the armed forces upon civilian informational structures. For example, about 95% of military communication occurs through civilian channels and many modern military crafts are designed using commercial software with blueprints kept in digital format on network-accessible platforms (Berkowitz 1997: 176).

According to Hundley and Anderson (1997: 238-9), there are five major types of computer crimes against which the American military-industrial complex must protect itself. These are, 1) *Operations-based attacks*, which involve gaining physical access to computers through illegal means, 2) *user authentication-based attacks*, in which perpetrators bypass password-protected systems, 3) *software-based attacks*, which involve exploiting software features such as "backdoors" or program flaws, 4) *network-based attacks*, which exploit network design or protocol, and 5) *hardware-based attacks*, by which the hacker exploits hardware flaws to disrupt computer systems.

Denial of service attacks, such as the ones perpetrated by the Electronic Disturbance Theatre (EDT), would fall beneath the network-based attacks and therefore be categorized as online crime. The exploits of the hacker cell *Kaotic Team* would also fall under this category, as would many political hacktivists using militant digital strategies for political ends. As the border between the civilian and military spheres blurs, a virtual revolution is occurring in civilian, military and intelligence circles to counter the looming

threat of computer "terrorism". By advocating a close relationship between civilian and military spheres, RAND proposes a system wherein the military-civilian communications grid is kept safe for use by both corporate and state interests through building safer network systems as well as keeping a close eye on the matrix for signs of potential malefactors.

4.4 The Echelon Project

Governments are also extending an invisible hand over cyberspace. In January 1998, a report was presented to the European Parliament entitled "An Appraisal of Techniques of Political Control" which stated,

> [w]ithin Europe, all email, telephone and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland via the strategic hub of London then by Satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York Moors of the UK. (Wright 1998: n. pag.).

The Echelon project, brainchild of the American National Security Agency, is composed of five intelligence agencies tied together through an alliance known as the UKUSA Signals Intelligence Agreement, which came into being in 1948 primarily to monitor radio transmissions emanating from the Soviet Union (Hager 1998). The agencies actively involved in this agreement, in addition to the NSA, are the Government Communications Headquarters (GCHQ) in the UK, the Communications Security Agency (CSA) in Canada, the Defense Signals Directorate (DSD) in Australia, and the Government Communications Security Bureau (GCSB) in New Zealand.

The difference between Echelon and other forms of contemporary espionage and surveillance is that it targets primarily non-military targets such as governments, organizations, businesses and individuals (Hager 1998: n. pag.). Through a series of powerful computers situated in recording stations around the world, such as the one at Menwith Hill, England, which sports 22 satellite dishes and 4.9 acres of terrain, intercepted communications are filtered through a series of "dictionaries" which scan the

messages for specific keywords (Hager 1998: n. pag.). Each agency has a different dictionary, which has secret lists of keywords reflecting the concerns and priorities of their respective governments. Should any of these keywords appear, the message is copied and re-routed to the proper channels for further investigation. For example, should a phone conversation intercepted by the Waihopai station in New Zealand include keywords listed in the Canadian CSA dictionary, it is rerouted to Ottawa without the New Zealanders reading it. In this manner, each one of the five major Echelon stations function as listening posts for the NSA, DSD, GCHQ, CSA, and GCSB intelligence agencies.

Echelon's surveillance systems operate on many different levels, the highest being the monitoring of international telecommunication satellites (Intelsats) used by most telephone companies around the world (Hager 1998: n. pag.). Through these, intelligence agencies can eavesdrop on tens of thousands of simultaneous telephone, fax and email communications in certain areas of Europe, Japan and South-East Asia. Other Echelon stations monitor communications not carried by Intelsats, with targets including Russia and Indonesia (a station at Leitrim, just south of Ottawa, is responsible for watching over Latin American communications). Land-based communications such as those carried through underwater cables and microwave stations are also monitored, leaving few rocks unturned.

In a report released by Statewatch, Echelon is decried as "a truly global threat over which there are no legal or democratic controls" (1997: n. pag.). In 1992, British intelligence agents told the London Observer that Echelon agents frequently monitored such organizations as Amnesty International and Christian Aid. As Hager attests,

> [t]he use of intelligence services in these cases had nothing to do with national security, but everything to do with keeping tabs on critics. The British government frequently finds itself in political conflict with Amnesty over countries it is supplying arms to or governments with bad human rights records. ECHELON provides the government with a way to gain

> advantage over Amnesty by eavesdropping on their operations (1998: n. pag.).

The breath of monitoring systems such as Echelon constitute a major threat to online activists, for it enables both state and private enterprises to monitor organizations deemed "hostile" and initiate steps to neutralize perceived threats in the shadow of the public eye. In this way, intelligence agencies can control and/or prevent activist groups from using the Internet as a communications medium. Through such strategies, these agencies can assume the power to monitor and censor cyberspace, thereby inhibiting the freedom of expression vital to online political discourse. In its set of recommendations, the Wright report stressed the necessity that,

> [a]ll surveillance technologies, operations and practices should be subject to procedures to ensure democratic accountability and there should be proper codes of practice to ensure redress if malpractice or abuse takes place. Explicit criteria should be agreed for deciding who should be targeted for surveillance and who should not, how such data is stored, processed and shared. Such criteria and associated codes of practice should be made publicly available. (1998: n. pag.)

Examples of such abuses could be monitoring individuals and organizations that, although not convicted of any crime, may nevertheless be deemed politically undesirable. If allowed to function without any sense of public accountability, such organizations and/or individuals could be silenced through such methods as intimidation, disinformation campaigns, or even the destruction or confiscation of their computer software.

4.5 Conclusion

As has been shown, the matrix is not beyond the reach of governmental, military and intelligence agencies. In this chapter, we explored online censorship through Libertarian theory and revealed how the US administration is trying to extend its power over the Internet. Moving on to network security and international surveillance, we explored how through such projects as Echelon, intelligence agencies could potentially monitor and/or

act against individuals or organizations for political reasons. If the matrix is to flower as a medium for political expression, we discussed, then the state must be closely watched so as to prevent it from extending arbitrary controls over the medium. This is not to say that the Internet should be haven for criminals and terrorists, for if a crime is committed then legal consequence must apply. What is of concern is the arbitrary silencing of activists for political reasons, not the legal pursuit of convicted or suspected criminals.

In the next chapter, we will explore in depth how a small guerilla movement from the southeast of Mexico has entered into the matrix and used it in their struggle for peace and human rights. Showing that the matrix still functions strongly as a social and political medium, the story of the Zapatista netwar presents us with an example of how a small and impoverished group were able to command worldwide attention through their use of information and communication.

Chapter 5

The Zapatista Netwar

5.1 Introduction

On New Year's Day 1994, a political earthquake erupted across Mexico. In the early hours of dawn, over two thousand members of the Zapatista National Liberation Front (EZLN) emerged from the Lacandona jungle, occupied six Chiapan towns, and declared war on the Mexican government. Having captured a radio station in San Cristobal, the EZLN sent their rebel message across the airwaves and initiated a digital campaign that was to grow into a global netwar. By gaining access to informational networks spanning the globe, the Zapatista were able to disseminate information quickly and efficiently, sidestepping traditional media. A war of guns had become of war of words fought across the nonspace of the matrix. In this chapter, the history of the Zapatista uprising will be analyzed within an informational context, concentrating on propaganda and information dissemination techniques. The factors involved in the creation of a global Zapatista movement will be discussed, as well as the cultural, social and political issues involved in the creation of this information war. Taking an historical perspective, this chapter will reveal how the EZLN is the latest in a long series of efforts at indigenous political organization and resistance. Furthermore, it will suggest how the Zapatista netwar grew out of inter-village communications networks, growing political awareness, and the building of close relationships with sympathetic Mexican and foreign human rights. Combined with examples of the EZLN's informational savvy, we will see how the Zapatista uprising evolved from a ground war into a digital one, and consider the impacts upon both the Mexican political fabric and online activism as a whole.

5.2 Chiapas: Poverty in a Rich Land

The province of Chiapas, situated on the Guatemalan border in the southeast portion

of Mexico, is extremely poor. As Elaine Katzenberger describes,

> [e]ighty percent of its municipalities are in a state of neglect classified by the Mexican government as "acute marginalization." Data for 1990 from the National Population Council show that out of a population of over 3.5 million, 30.1 percent are illiterate, while 62.5 percent did not finish their primary education.... More than 35 percent of the state's dwellings lack electricity or drainage while 51 percent have earthen floors and 70 percent are overcrowded. Nineteen percent of the working population receives no income and nearly 40 percent receives less than the daily minimum wage [11 pesos, roughly $3.00 per day], while 21.2 percent receives between one and two minimum wages. (1995: 33)

This state of extreme poverty is ironic when one considers the great natural wealth within the province's borders. Unlike other Mexican provinces, writes Subcomandante Marcos, military leader and star spokesman for the EZLN, Chiapas is "an internal colony" (Marcos 1994: n. pag.) dominated by a wealthy Mexican elite and serving as a source for natural resources and cash crops upon which Mexico's economy depend. In a work entitled "Chiapas, The Southeast in Two Winds: A Storm and a Prophecy," Marcos describes not only the province's rape at the hands of the state, but also underscores the role played by transnational corporations operating in its oppression. The Maya and other native groups in the area have not been isolated from the rest of the world, for they have suffered at the hands of corporations intent on exploiting their resources in the name of profit. The recent emergence then of the Zapatista netwar can be seen as a different form of interaction with the international community, one based on action and cooperation rather than oppression and exploitation. The global community has been involved with Chiapas for a long time, and through the netwar has begun to realize its responsibilities and the debt owed to the aboriginal peoples of this province.

> Chiapas loses blood through many veins: Through oil and gas ducts, electric lines, railways, through bank accounts, trucks, vans, boats and planes, through clandestine paths, gaps, and forest trails. This land continues to pay tribute to the imperialists: petroleum, electricity, cattle, money, coffee, banana, honey, corn, cacao, tobacco, sugar, soy, melon, sorghum, mamey, mango, tamarind, avocado, and Chiapaneco blood flows as a result of the thousand teeth sunk into the throat of the Mexican

> Southeast. These raw materials, thousands of millions of tons of them, flow to Mexican ports and railroads, air and truck transportation centers. From there they are sent to different parts of the world: The United States, Canada, Holland, Germany, Italy, Japan, but with the same fate—to feed imperialism. The fee that capitalism imposes on the Southeastern part of this country oozes, as it has since from the beginning, blood and mud. (Marcos 1994: n. pag.)

Harry Cleaver, Professor of Marxist Theory at the University of Texas at Austin, has been studying the Zapatista since early 1994. In an essay entitled "The Zapatistas and the Electronic Fabric of Struggle," he explores the links between Chiapas and the global, capitalistic corporate society.

> Chiapas has been an integral part of Mexican and global capitalism for a long, long time. The workers of Chiapas have provided the rest of Mexico and the world with agricultural exports such as lumber, coffee and beef and their own labor power through migration north. For quite some time, they have also been providing hydroelectric power and oil, essential components of "modern" Mexican industrialization. Locally, they have labored in that most contemporary sector of post-industrial society –the tourist industry—providing the services required, and coming into constant contact with people from all over the world. (1995: n. pag.)

Having for so long been the victim of global greed, Chiapas was already a prominent actor on the world stage. That its struggle for survival would also be waged before the eyes of the international community seems but a continuation of the close relationship between Chiapas and the global village.

5.3 A History of Resistance

The Zapatista uprising was the latest in a long series of attempts at popular organization, and therefore must be perceived as part of a complex mosaic rather than an isolated, spontaneous incident (Collier 1994). The beginnings of contemporary Chiapan political organizing can be traced, perhaps surprisingly, to the activities of Protestant and Catholic missionaries. In an effort to loosen the grip of the Catholic Church upon much of the Chiapan population, the Protestants attempted to attract more converts by preaching in indigenous languages rather than Spanish. The impact of this

strategy was profound, for it

> ... not only helped make the nontraditional churches more accessible, but also helped empower Indians who previously were forced to suffer the indignity of being treated as second-class citizens even in Church, where the Catholic priests administered the sacraments only in Spanish. And although Chiapas does have a high literacy rate compared with the rest of Mexico... census statistics show that literacy rates are higher in native-language speaking communities that are Protestant.... As literacy is freed from its repressive political context, Mexican politics becomes more accessible because peasants no longer fear that it will destroy their traditions. (Collier 1994: 58)

In addition to the "decolonizing" of language, the impacts of grassroots proselytizing included the creation of a powerful feeling of community amongst the *Indigena*. Collier, on a visit to the Chiapan village of Sekemtik, describes how the Protestant approach "forged a bond of affinity among the residents of this community, [drew] women and children as well as men into a vibrant congregation, [created] a space in which people could challenge the boundaries not just of gender and literacy, but of access, through literacy, to formerly impenetrable domains of law and politics" (1994: 59).

The Catholics, perhaps feeling threatened by the Protestants' popularity, soon adopted the same grassroots strategies which had so well served their opponents. In 1974, Bishop Samuel Ruiz organized an Indigenous Congress in memory of Fray Bartolomé de las Casas, a sixteenth century champion of indigenous rights (Collier 1994). The aim of the congress was to give voice to those whom before had been denied, thereby creating a closer relationship between the Church and its congregation. "[I]f the church does not make itself Tzeltal with the Tzeltales, Ch'ol with the Ch'oles, Tojolabal with the Tojolabales, I don't understand how it can call itself the Catholic Church," Ruiz said. "It would be, in effect, a foreign church, belonging to a dominant social class" (Qtd. in Hermosillo 1995: 72).

The impact of the Indigenous Congress strengthened the process of grassroots organization, soon leading to discussion and debate over issues of land, food and

education, issues which later became battle cries for the EZLN (Collier 1994). Catechists traveled to Chiapan communities, teaching courses in native languages as well as history, political economy and Mexican commerce. It also helped build a "jungle network" between people from different communities, thereby establishing channels of communication that would later serve to create and maintain alliances. By 1978, a movement called *Política Popular* had taken over from the Church as central organizers in eastern Chiapas, thereby displacing the focus of popular organization from the religious to the secular realm.

When the oil prices collapsed in 1982, Mexico's sudden inability to repay its staggering foreign debt undermined the international banking system and seriously threatened further investment into the country (Collier 1994). As the debt crisis of the 1980's and 90's worsened and state oppression of the *campesinos* intensified, concentrated efforts were made to establish inter-community links as well as building relationships within developed networks of communication and mutual aid both in and out of Mexico. The result was the creation of a comprehensive web of sympathetic organizations, many of which had already built a complex infrastructure in their fight against the North American Free Trade Agreement.

It was this web of sympathetic individuals across the world that was to become the foundation upon which the Zapatista netwar would be built. Starting with the creation of jungle networks between different Chiapan villages and the emergence of political consciousness partly as a result of the Protestant and Catholic influence, Chiapans extended their network to organizations beyond their borders. Following the 1994 uprising, these networks of support exploded into action, effectively catapulting a land war into cyberspace.

5.4 The Two Mexicos

In an interview with reporter Medea Benjamin, Marcos explains how one of the

challenges facing the Zapatista in their quest for international recognition was the propaganda campaign waged by the Mexican government in order to improve its image in the eyes of United States as well as other potential investors (Benjamin 1995: 58). Despite long-standing agrarian and human rights issues not only in Chiapas but across Mexico, reports of brutality, and widespread political corruption, the official state position was one of denial and reassurance that all was well in the country. Although the state had been aware of guerilla activity in Chiapas for some time, for example, they attempted to downplay the crisis in the hope that it would escape both domestic and foreign eyes.

> In May 1993, the army had raided an EZLN garrison in the remote colony of Corralchén. Although first reports described the raid as having routed out a guerrilla camp, complete with underground bunkers and a scale model of the municipal headtown of Ocosingo, the government subsequently downplayed the reports. At the time, acknowledging the existence of a guerrilla movement in Chiapas would have endangered the chances that the US Congress would accept NAFTA, as it finally did after a battle hard fought and won by U.S. President Bill Clinton in the summer of 1993. (Collier 1994: 86)

Faced with the Mexican government's efforts to conceal and isolate the Zapatista uprising from the rest of the world, thereby denying the guerrillas the possibility of foreign support, the EZLN realized that in order to succeed they would have to break down the wall of silence. As Marcos describes,

> [t]he [Mexican] government has tried to portray Mexico as a First World country. They want to show the World Trade Center, the big malls, the Zona Rosa, the big, modern cities- Acapulco, Cancun, Mexico City. Monterrey, Guadalajara. They want to show the tourists the lovely Mexican culture- the mariachis, the folkloric dancing, the beautiful clothing and crafts of the indigenous people. But behind this picture is the real Mexico of the millions of Indians who live in extreme poverty...We have helped peel off the mask to reveal the real Mexico. Our uprising was the only way to draw world attention to the poverty and injustices that the indigenous people have been suffering for over 500 years. (Qtd. in Benjamin 1995: 58)

Human rights reports such as those compiled by Amnesty International (1998) support Marcos' statement with reports of rampant torture, corruption and frequent

human rights violations. Human Rights Watch, furthermore, describes the Mexican government as paying "rhetorical attention to human rights" (HRW 1998: n. pag.), stating how

> [a]uthorities failed to address human rights violations stemming from acute rural tensions, the army's confrontation with leftist guerrillas, and a much-needed but ill-designed campaign to fight organized and common crime. In case after case, Mexican officials refused to engage in constructive dialogue with Mexican and international human rights organizations, preferring to obfuscate or ignore human rights issues rather than offer workable solutions to well-documented problems. At the heart of many abuses lay Mexico's police and justice systems, which often functioned at the expense of, rather than in support of, human rights." (1998: n. pag.)

Paramilitary groups, also known as death squads, pose serious problems in Mexico, particularly in rural provinces such as Oaxaca and Chiapas. Generally hired gunmen equipped by local ranchers and landowners, they terrorize the *campesinos* so as to short-circuit any attempt at political organization. On December 22, 1997, a small Chiapan town became the scene of a brutal massacre when a PRI-supported death squad opened fire on a crowd of mostly women and children, alleged EZLN supporters, who had gathered in the village church. As an essay posted on a Zapatista web site described how

> ... a group of 60-70 members of a PRI-backed paramilitary group .... descended upon the Tzotzil village of Acteal... where hundreds of displaced Zapatista supporters and members of the peaceful civilian organization known as "Las Abejas" had taken refuge.
>
> The attackers were armed ... [with] weapons which they could only have obtained from military or police sources. They opened fire on the village as many of its inhabitants where attending church services and praying for peace and reconciliation in the municipality.
>
> The slaughter continued as hundreds of people ran toward a nearby river in a vain effort to escape. 45 people were killed during the attack (21 women, 14 children, one infant, and 9 men), and more than 25 others were wounded. The bloodbath lasted five hours, during which time the Public Security police stood by--some no more than 200 meters away--and refused to intervene (1998: n.pag.)

5.5 Digital Zapatismo

When the Zapatista emerged from the jungle on January 1, 1994 and declared war on the Mexican government, they were ready for a fight. However, in addition to the importance of military organization and efficiency on the battlefield, Marcos also realized the power of the media as a parallel strategy to violence, and tailored his message accordingly with skill and insight. In an interview given to the Mexican journal La Jordana on January 19, 1994, Marcos describes the reasons for the uprising,

> We cannot let ourselves be treated this way, and we have to try to construct a better world, a world truly for everyone, and not only for a few, as the current regime does. This is what we want. We do not want to monopolize the vanguard or say that we are the light, the only alternative, or stingily claim the qualification of revolutionary for one or another current. (Marcos 1994)

Unlike some previous revolutionary movements, the Zapatistas did not claim to want to take power for themselves (Benjamin 1995). As Marcos affirms,

> There's a big difference between the guerrilla movements of the fifties, sixties, and seventies, and [the Zapatistas]. Before, they said, "Lets get rid of this system of government and put in another kind of system." We say, "No, the political system can't be the product of war." The war should only be to open up space in the political arena so that the people can really have a choice. It doesn't matter who wins, it doesn't matter if it's the extreme Right or the extreme Left, as long as they earn the confidence of the people.... We want to create the political space, and we want the people to have the education and the political maturity to make good choices. (Qtd. in Benjamin 1995: 61)

In his classic treatise *On War*, Carl Von Clausewitz asserts that "the aim of warfare is to disarm the enemy..." (1976: 77). The process of disarming, however, has traditionally been carried out in a violent manner. When the Zapatista attacked on January 1st, 1994, they expected the Mexican army to retaliate in force, probably resulting in many deaths including all of the officers involved in this first strike.

> ...[A]ccording to our organizational concept, the leaders must lead the troops in combat, in order to have moral authority. But we thought that the first string of leaders would be killed in the first days of combat. We thought that all of us leading the troops would die... So then what happened? We went out, we fought, and they didn't kill us. That's the

> great surprise, that they didn't kill us that first week of January. (Qtd. in Benjamin 1995: 65)

The reason for the sudden cease-fire and the initiation of negotiations between the Zapatista and the Mexican government was the sudden domestic and international outcry immediately following the outbreak of hostilities (Peña 1995: 96). Although the Zapatista themselves were expecting a more traditional military operation, the media storm following their attack was no accident. In addition to building networks of support across Cyberia, the Zapatista had also targeted the local and international media they felt would be sympathetic to their cause. As Peña explains,

> [Marcos] planned his relationship with the media very carefully. The international press was a priority, of course. *Der Spiegel*, *Cambio 16*, *Le Figaro*, the *New York Times*, the *San Francisco Chronicle*, *NACLA*, and *Vanity Fair* were immediately welcomed into the jungle. In regards to the Mexican press, he was a bit more cautious. He favored the two independent dailies, *La Jordana* and *El Financiero*, and developed a direct line of communication with them. He also put a lot of emphasis on radio, since for most of the indigenous communities of Chiapas and throughout rural Mexico it is the main source of information. (Peña 1995: 91)

Through this close relationship with not only the digital media but print and radio as well, the Zapatista initiated an information war following what Richard Szafranski termed *neocortical warfare* (1997). Outgunned as they were on the ground, the Zapatista gained an advantage by winning the hearts of many Mexicans and foreigners alike through their superior use of public relations and strategically sound pieces of information releases at planned intervals to specific venues. Instead of following Von Clausewitz's contention that the best way to subdue an opponent is through violence, the Zapatista were quick to recognize this new form of power.

Szafranski's definition of power, a view which coincides well with the EZLN's informational strategy, involves the ability to subdue the opponent's will, preferably through non-violent means (Szafranski 1997: 397). Sun Tzu, the great Chinese general of the Han period, asserted that "the skillful leader subdues the enemy's troops without

any fighting; he captures their cities without laying siege to them; he overthrows their kingdom without lengthy operations in the field" (Sun Tzu n.d.). The notion of "subduing without fighting" is the cornerstone of Szafranski's vision of "neocortical warfare," which involves not "the application of physical *force*, but ...the quest for metaphysical *control*" (1997: 399).

But how can metaphysical control be achieved through information warfare? According to John Arquilla, this would involve,

> ... trying to disrupt, damage or modify what a target population "knows" about itself and the world around it... It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception of or interference with local media, infiltration of computer networks and databases, and efforts to promote a dissident or opposition movements across computer networks. (1997: 28)

The EZLN's tearing away of the Mexican's government's mask of stability and wealth it tried to present to both its own citizens and the global community is an example of information war for, as Arquilla states above, it undermines the beliefs and assumptions of the target population. Rather than the image of art and culture and rich natural resources that the state offered as the Chiapan reality, the EZLN presented the world with pictures of death, oppression and disease. Furthermore, Marcos' refusal to identify with any established Western political movement fit in well with the global nature of information warfare. By appealing to universal desires such as freedom from oppression, health, education and the right to self-determination, while avoiding Western political labels, the EZLN managed to establish a wide support base, effectively cutting across culture, race and language.

As Guillermo Gómez Peña observes,

> In the confusing era of "the end of ideology," [Marcos'] utopian political visions - presented in simple, nonideological, and poetic language – went straight to the jaded hearts and minds of students, activists, intellectuals, artists, nihilistic teens, and even apolitical middle-class professionals. In an era of ferocious neonationalisms, he made sure to avoid nationalist jargon and dogmas. His combination of political clarity, bravado, and

> humility appealed to progressive politicians and activists throughout the world. (1995: 90)

The extent to which Digital Zapatismo spread across the world is seen in the extensive support they received following the massacre at Acteal on December 22, 1998. Detailed eyewitness reports were circulated daily and posted on web sites such as the *Zapatista Army of Liberation* (http://www.peak.org/~joshua/fzln). A list of the names of all who had died was posted to the site, followed by exhortations to act now by taking to the streets, writing letter and/or emails (address and phone numbers of US and Mexican governments were provided). A letter sent out on the Chiapas95 mailing list on January 5, 1998, provided a comprehensive list of Mexican embassies in the U.S. including street address, phone, fax and, where possible, email addresses, while others included an electronic petition to be sent to Mexican President Zedillo.

As Cleaver describes,

> First through written communiqués and personal interviews with independent journalists which were flashed around the world by fax and electronic mail, then through more detailed reports by Mexican and foreign observers circulated in the same manner, the Zapatistas were able to break out of the state's attempted isolation and reach others with their ideas and their program for economic and political revolution. As vast numbers of Mexicans responded with sympathy and mobilized in support, the Chiapas uprising kindled a more generalized pro-democracy movement against the centralized and corrupt Mexican economic and political system. Inspiring many others outside of Mexico, the Zapatista uprising set in motion a new wave of hope and energy among those engaged in the struggle for freedom all over the world. (1995: n. pag.)

In the 23 days following Acteal, there were over 230 actions undertaken in support of the Zapatistas in 130 cities in 27 countries across 5 continents (Wray 1998: n. pag.). Over 160 thousand people were involved in these actions, emphasizing the degree to which the Zapatista cause has spread across the globe. On January 9, 1998, Eduardo Vera, from the *Comite de Solidaridad Con Chiapas y Mexico*, sent an email on Chiapas 95 declaring that Austin (TX) supporters of the Zapatista would join in a worldwide day of protest on January 12th designed to bring attention to the plight of Chiapas and stop

American military aid to Mexico. Statistics subsequently released on Chiapas 95 revealed that on January 12, eighty public demonstrations, vigils, sit-ins, blockades and celebrations were held in support of the Zapatista in cities across the United States, Canada, France, Greece, Switzerland, Spain, Portugal, Holland, Ireland, Italy, Japan, Argentina, Puerto Rico, Costa Rica, Ecuador, Uruguay, Bolivia, Honduras, El Salvador, Nicaragua, Cuba and Mexico. Among the largest international demonstrations was one in Madrid, Spain, where between 3,000 and 5,000 people assembled before the Mexican consulate. In Mexico City, 80,000 to 100,000 people assembled in the Zocalo (central plaza) to voice their disapproval of the situation in Chiapas. The sheer number of people involved in these public manifestations of support, all occurring on a single day, suggests widespread organization and cooperation spanning borders and continents. Such a degree of cohesiveness, one may suggest, would have been hard to achieve without the existence of computerized networks of alternative communication.

Cleaver, in his essay "The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric" (1997), notes how prevalent support for the guerrillas was amongst indigenous, environmental and feminist groups. As discussions about the possibilities of alternative political and social approaches to state policy become more prevalent in cyberspace, differing viewpoints such as the ones suggested by the Zapatistas gain a credibility that would have been hard to achieve outside of such a critical environment. As Cleaver discusses,

> The co-existence and interconnections among these [political critiques and experimentation on the Internet] was obvious at the Zapatista-called meetings and continues to be discussed in cyberspace. Important in these discussions have been the experiences of indigenous peoples in seeking ways to organize democratic spheres of political interaction among diverse cultural, ethnic and linguistic communities without dissolving their differences... These indigenous experiences have had wider influences not only because the Zapatistas have brought them to other's notice – but because these efforts have actually been successful at building networks among a diverse array of indigenous peoples.... The indigenous demands for autonomy have resonated within a wide variety

of ethnic and linguistic and linguistic communities. (1997: n. pag.)

Inspired by the Zapatistas, numerous grassroots organizations have since challenged the party-state and/ or withdrawn their support of the government. Accusations of economic inequality, human rights abuses and media manipulation have increased, as well as popular unrest and disillusionment with the political situation. Although a covert campaign of low-intensity warfare still continues in Chiapas, the ability of the Zapatista, through their online campaign, to focus public attention on the state's actions have seriously hampered the state's ability to unilaterally crush their opposition, and may have even sparked the beginnings of fundamental political reform. This may herald a new era in international activism, for now information is in the hands of those wi[illegible]nd able to use digital networks to their own advantage. As the Zapatista experience shows, states can no longer easily isolate and crush wired opponents without risking intense international critique.

5.6 Conclusion

Although they may not have realized it at the time, on January 1st, 1994, the Zapatista heralded a new age for digital activism. The most recent in a long history of organization and resistance, the Zapatista rose from a small socialist revolutionary cell to become an indigenous army which challenged the might of the Mexican state and lived. Through media savvy and brilliant soft power strategy, the Zapatista wove extensive webs of resistance and cooperation that in turn put Chiapas on the international activist map. By carefully crafting his words so as to avoid easy political labeling and appealing to liberal ideals such as the right to education, health and self-determination, Marcos cut across cultures and language. "Digital Zapatismo" spread from countries such as the United States, Spain, France and Japan, causing not only a tidal wave of support but also sparking the birth of other activist groups which believed in the Zapatista ideals and saw the EZLN's struggle as being more than a Mayan or indigenous struggle. Through their

netwar, the EZLN captured the hearts and minds of people the world over, and although the killing and oppression still continues in Chiapas there is a glimmer of hope in the fact that the government did initiate negotiations with the Chiapans, using words when only days earlier they had used guns.

Conclusion

So as angry Arachne wove her webs, her progeny spread out upon her silk tapestry, weaving their own webs of resistance and action in the face of states and corporations. Despite the efforts of sword-wielding Athena, small, fast and highly flexible info warriors are using cyberia to communicate, organize and consolidate their common strengths. First among Arachne's children are the EZLN, whose skillful use of soft power in their struggle for human rights in their home province of Chiapas heralded a new era in digital warfare. Through their star-spokesman Subcomandante Marco as well as others, the EZLN waged a new revolution both on the ground and on the Net. Unlike previous revolutionaries whose purpose was to overthrow the reigning political regime and replace it with one of their own choosing, the EZLN offered no such easy solutions.

Avoiding typecasting by refusing all political identification, the indigenous rebels challenged the world to find a solution to the problems of aboriginal poverty and oppression not just in Chiapas but worldwide. As a result, the struggle of the Zapatista was identified as part of a greater struggle encompassing such issues as the environment, indigenous rights, agrarian reform, labor rights and women's rights. Through their skillful use of established activist networks, they were able to capture the attention of academics, students, workers, feminists, socialists and indigenous workers, thus making the Zapatista struggle a symbol of the pre-millennium fight against global corporate exploitation. The EZLN came to symbolize the poor and dispossessed who did not figure in the economic rationale fueling many of the globalization debates. The result was a global uproar loud enough to silence the guns of war and bring about negotiations between the Zapatista and the Mexican state.

From its first steps as a secret government-funded project to a global informational grid, the matrix has asserted itself as not only a new means of mass communication but

also a cultural medium distinct from the Western military agencies that spawned it. Based upon anarchistic principles of diversity and self-regulation, the Internet provides a political and social medium where discourse flourishes and a high level of alternative political consciousness strives. This is not to suggest that the Internet is part of a worldwide anarchist movement or that the medium somehow promotes a transition to anarchy, however, but suggests that the physical and societal structure of the medium is best represented through the anarchist model. Due to a lack, at the present time, of any central authority, the Internet serves as home to peoples of all political persuasions, from the capitalist to the socialist to the indigenist. Thus providing the environment for the flowering of political discourse, the anarchistic system acts as a vehicle for freedom of expression but, in itself, imposes few constraints upon what such expression would be.

Ushering in a new age of digital existence, cyberspace offers new challenges, new opportunities, as well as unique perils which must be addressed in order to fully understand the impact the existence of cyberia has had, and will continue having, on not just the Northern but Southern hemispheres as well. With its potential for creating networks of communication independent of either borders or geographical space, the Internet offers new avenues for the growth of new communities and the exchange of ideas and worldviews. Through the offering of alternative, unregulated sources of information, the Internet offers citizens access to uncensored information right from their computers.

One of the principal opportunities offered by this digital realm is the application of soft power strategies. Soft power, the informational strategy central to any netwar campaign, combines public relations, the strategic use of information, charisma and cultural awareness. Unlike hard power, which targets the body of the opponent through violence, soft power affects the mind of the target. As in the realm of advertising, soft power works best without the target being aware that he/she is being influenced. Through the use of

soft power, netwarriors can work to sway public opinion and undermine state-sanctioned information, thereby motivating the individual to subscribe to the activist view and join the campaign. The Zapatista, who carefully tailored their political message in order to appeal to as wide and heterogeneous audience as possible, understood the importance of public relations skills and used it to great effectiveness in their campaign against the Mexican state.

As these analyses showed, soft power has many faces and can be used to enhance human interaction as well as to isolate and destabilize. As one of the core strategies employed by the Zapatista, soft power enabled the revolutionary group to garner support across the world and focus the public eye upon their impoverished province. Through the effective use of information and communications networks, the Zapatista did much to undermine the Mexican government's propaganda machine by reaching out with their own versions of events. In contrast to their military campaign, which would have been unlikely to succeed against the might of the Mexican army, the Zapatista's use of soft power proved to be one of their most successful strategies.

Canadian, American and European governments are also greatly aware of the potential for online social activism, however, and are taking steps both to monitor and protect against netwarriors. Analyzed through Libertarian theory, US attempts to control and censor the Internet were discussed and the potential threat they pose to political discourse online ascertained. Concerned with their lack of control over cyberspace and the relative vulnerability of the civilian communications grid, both governments and military agencies have been taking actions to counter the perceived threat. This fear of the unknown which seems to permeate state policy regarding online activism is revealed in the writings of military analysts advocating an organizational revolution in US military and intelligence circles in order to better prepare for the digital battlefield. These reports have a twofold approach, emphasizing the importance of developing efficient strategies

for both offensive and defensive scenarios. By combining superior systems and digital defense networks with aggressive cyberwar strategies, certain analysts advocate the development of effective digital warfare methods within a sound organizational framework, effectively making information warfare an integral part of the country's comprehensive defense policy.

Such a move would have a significant impact on online activists, for it could well undermine much of the informational advantages presently enjoyed by netwarriors such as the Zapatista and the American Indian Movement. Although at this time the hierarchical structures and top-down command frameworks of government institutions may hamper their performance online when faced with smaller, highly flexible and dynamic activist cells, the creation of specialized military and intelligence agencies dealing with both netwar and cyberwar scenarios would have a profound effect on the digital scene. For instance, intelligence agencies skilled in disinformation could use email lists to sow confusion and conflict within an activist ring, thereby eroding its internal cohesion and undermining its effectiveness. State sanctioned information could be disguised as originating from activist sources, thereby discrediting these sources and encouraging uncertainty as to what information is "correct".

Although from an activist perspective the adoption of netwar strategies by powerful and well-funded intelligence agencies may threaten the informational advantage presently held by netwarriors, it cannot be said that the weapons of soft power should be granted to one side but denied the other. The digital battlefield is an open one where victory goes to the swift, the flexible and the insightful. Should the state adopt a policy of information warfare strategy then cyberia would become much more complicated, and netwar a much more challenging endeavor for info warriors. Unlike previous communications monitoring schemes, projects such as Echelon target primarily non-military targets such as private companies, non-governmental agencies and individual

civilians. The implications for practitioners of information warfare are great, for they tear away the sense of privacy and anonymity that gives the matrix its activist potential. Email would become a far less reliable medium, communications networks could be exposed and wired activists monitored. Since one of the greatest strengths of information warfare is its ability to move large amounts of information quickly and without trace, the state's use of such a comprehensive online monitoring system as part of an informational strategy would result in its becoming a potentially powerful force on the digital battlefield.

In the case of the Zapatista, for example, should the Mexican government have developed netwar capability, it could have identified the Zapatista's initial attempts at building the networks that would eventually make the netwar possible and move to counter them through its own disinformation campaign aimed at discrediting the Zapatista and their followers. Although the Mexican government had launched a smear campaign in the regular media trying to depict the Zapatista as terrorists and drug smugglers, their lack of credibility in most activist circles and near-total absence on the online realm led to an online victory by the sophisticated and brilliant Zapatistas. Crippled by the undermining of its credibility by both the Zapatista and their followers, the Mexican administration found itself largely unable to counter the soft power attacks of the Zapatista and therefore lost the online public opinion war. Had the state access to the same political, psychological and technical tools that the Zapatista and their supporters enjoyed, the netwar may have been less clearly defined, and the Zapatista less at an advantage. This is cause of concern for contemporary activists, and further reason for them to maintain a close vigilance on the state as well as maintaining sound technical and political netwar strategies.

Despite the informational advantages that could be gained through the development of an info war strategy, however, the state appears to be more concerned with the direct physical monitoring and control of political groups rather than playing the soft power

game. Although Echelon could also become a formidable netwar weapon, it is the opinion of the author, based on many articles published by both RAND and the US military, that should action be brought against political activists it would be through the direct use of hard power rather than soft power. As was showed in such campaigns as Operation Sundevil, the state has shown itself ready to take direct physical action against politically suspect individuals, eliminating their access to online communication through either the confiscation of their computer equipment or the canceling of their online access through subversion and intimidation. In this way, the state can control and/or prevent activist groups from using the Internet as a communications medium. Thereby assuming the power to monitor and censor cyberspace and inhibiting the freedom of expression vital to online political discourse, the state appears to be setting itself up as a monitor of not only what can de done, but also what can be *said*. This merits close scrutiny, for should the state feel free to act against political activists online then we could potentially witness the arbitrary silencing or harassment of activists and other actors on the political scene.

As was discussed, in the case of the Zapatista and the American Indian Movement information warfare offers possibilities for action previously unknown. The practical importance of recognizing the existence of the Internet and its potential as a networking activist medium for both state and non-state actors is profound, for it poses a challenge to previously held notions of information and mass participation. The unhierarchical structure of the Internet subverts established institutions by favoring small, semi-independent cells functioning via coordination rather than control patterns. Through its rizomatic and fluid communication networks, the matrix offers what may be described as a functioning, global anarchist medium largely free from any central power or governing agency and molded according to the desires and convictions of its constituents.

Although there is a growing awareness in academic as well as military and intelligence circles as to the potential of netwar for challenging the existing power structure, most of the research presently being done appears to concentrate on cyberwar, aggressive hard power uses of computer technology, rather than the more soft-power oriented netwar. As I discussed in this thesis, I believe that online soft power strategies offer the greatest promise for online activists in that they expand their ability to disseminate information and convert others to their point-of-view. The importance of this research, therefore, lies in introducing the topic of soft power and information warfare within the anarchistic realm of the Internet. The implications of this will be divided into two categories: future academic research, and practical applications. The repercussions of this work on the academic field will be to stimulate a deeper analysis of how anarchism functions online and how this relates to the dynamic social and political structures of cyberspace. Furthermore, the developing concept of soft power may offer a radical redefinition of power both on the domestic and the national scene. Concentrating on the online medium, the linking of soft power with anarchism may offer new fields of study involving new perspectives on social political interpretations of the relationship between power and information. Finally, the cultural impact of increased access to information, particularly in the activist field, may result in more pressure being placed upon governments by the populace. This may lead to shifts in public policy, as well as a redefining of the relationship between the state and the people, particularly in democratic countries.

With regards to the practical aspects of my research, the Internet has proven itself an efficient medium of communication and therefore should be considered as part of most social and political activists' tool-kits. Individuals concerned with such issues as human rights, the environment, civil liberties, indigenous rights and women's rights should learn

Internet technology and make sure they maintain an online presence. Furthermore, those involved in social and political activism should consider the power of the network system and thrive to build and maintain communications networks with other like-minded individuals. The matrix is still in its infancy, and it will be exciting to participate in its unfolding as an educational, political and organizational medium.

Bibliography

Agencia Latinoamericana de Información (ALI) Home Page. Nov. 1998 <http://www.ecuanex.apc.org/alai/indexeng.html>.

Association for Progressive Communication (APC). "About APC." May 1999: <http://www.apc.org/english/about.html>.

- - -. "A Brief History of the APC." May 1999: <http://www.apc.org/english/msjob.html>.

- - -. "Mission Statement." Nov. 1998: <http://www.apc.org/about.html>.

Amnesty International. "Annual Report 1998: Mexico." Dec. 1998. <http://www.amnesty.org/ailib/aireport/ar98/amr41.htm>.

Annis, Sheldon. "Giving Voice to the Poor." Foreign Policy 84 (1991): 93-106.

Arquilla, John. "The Great Cyberwar of 2002." Wired Feb. 1998. Feb. 1999 <http://www.wired.com/wired/archive/6.02/cyberwar.html>.

Arquilla, John and David Ronfelt, eds. In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA: RAND Corporation, 1997.

Bakel, Rogier V. "How Good People Helped Make A Bad Law." Wired Feb. 1996. Feb. 1999 <http://www.wired.com/wired/archive/4.02/digitel_pr.html>.

Barber, Benjamin R. Jihad vs. McWorld. New York: Ballantine, 1995.

Barlow, J.P. "Jackboots on the Infobahn." Wired Apr. 1994. Feb. 1999 <http://www.wired.com/wired/archive/2.04/privacy.barlow_pr.html>.

Benjamin, Medea. "Interview: Subcomandante Marcos." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 57-70.

Bennahum, David S. "The Hot New Medium is... Email." Wired Apr. 1998. Oct. 1998 <http://www.wired.com/wired/6.04/es_lists.html>.

Berkowitz, Bruce D. "Warfare in the Information Age." In Athena's Camp: Preparing For Conflict In The Information Age. Eds. John Arquilla and David Ronfelt. Santa Monica, CA: RAND Corporation, 1997. 175-189.

Berners-Lee, Tim and Robert Cailliau. The World-Wide Web. Jan. 1992. Oct. 1998 <http://www.w3.org/talks/general.html>.

Besser, Howard. "From Internet to Information Superhighway." Resisting the Virtual Life. Eds. James Brook and Iain A. Boal. Monroe, OR: City Lights, 1995. 59-70.

Bookchin, Murray. "The Anarchist Revolution." Contemporary Anarchism. Ed. Terry M. Perlin. New Brunswick, NJ: Transaction, 1979.

Bookchin, Murray. The Ecology of Freedom: The Emergence and Dissolution of Hierarchy. Montreal, QC: Black Rose, 1991.

Bookchin, Murray. Post-Scarcity Anarchism. Montreal, QC: Black Rose, 1986.

Cailliau, Robert. A Little History of the World Wide Web. Oct. 1995. Oct. 1998 <http:// www.w3.org/talks/general.html>.

Canada. Dept. of Foreign Affairs and International Trade. Canada and Human Security: The Need for Leadership. By Lloyd Axworthy. 1998. 2 November 1999 <http:// www.dfait-maeci.gc.ca/english/foreignp/sechume.htm >.

Chomsky, Noam. "That's a Little More Information than I Need to Know, or Information Anarchy and the Plight of the Igno-rant." The Noam Chomsky Archive.1995. 2 November 1999. < http://www.zmag.org/chomsky/index.cfm>.

Chomsky, Noam. "Time Bombs." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 175-182.

Churchill, Ward. "A North American Indigenist View." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 141-155.

Clark, Nigel. "Earthing the Ether: The Alternating Currents of Ecology and Cyberculture." Cyberfutures. Eds. Ziauddin Sardar and Jerome R. Ravetz. New York: New York UP, 1996. 90-110.

Cleaver, Harry. The Zapatista and the Electronic Fabric of Struggle. Nov.1995. 10 September 1998 <http://www.eco.utexas.edu/faculty/Cleaver/zaps.html>.

Cleaver, Harry. The Zapatista Effect: The Internet and the Rise of an Alternative Political Fabric. Nov. 1997. 10 September 1998. <http://www.eco.utexas.edu/faculty /Cleaver/zapeffect.html>.

Collier, George A. Basta! Land and the Zapatista Rebellion in Chiapas. Oakland, CA: Food First, 1994.

Davis, Norman C. "An Information-Based Revolution in Military Affairs." In Athena's Camp: Preparing for Conflict in the Information Age. Eds. John Arquilla and David Ronfelt. Santa Monica, CA: RAND Corporation, 1997. 79-98.

Docherty, Alan. "Net Journalists Outwit Censors." Wired 13 March 1999. Nov. 1999 <http://www.wired.com/news/politics/0,1283,18435,00.html >.

Dolgoff, Sam. "The Relevance of Anarchism to Modern Society." Contemporary Anarchism. Ed. Terry M. Perlin. New Brunswick, NJ: Transaction, 1979.

Electronic Disturbance Theatre (EDT). Chronology of SWARM. Nov. 1998 <http://www.nyu.edu /projects/wray/CHRON.html>.

Electronic Frontier Foundation (EFF). "Mission." 20 May 1999 <http://www.eff.org/ EFFdocs/about_eff.html#mission>.

European Parliament. Directorate General for Research: Directorate B. An Appraisal of Technologies for Political Control. By Steve Wright. Ed. Dick Holdsworth. 6 January 1998. Feb. 1999 <http://www.jya.com/stoa-atpc.htm>.

Exon, James. "Keep Internet Safe for Families." CyberReader. Ed. Victor J. Vitanza. Needham Heights, Mass: Allyn & Bacon, 1996. 155-156.

EZLN: Zapatista Front for National Liberation. First Declaration of the Lacandona Jungle. 1993. Dec. 1998 <http://www.peak.org/~joshua/fzln/1st-decl.html>.

Gibson, William. Neuromancer. New York: Ace, 1984.

Glave, James. "Cyber 'Vandals' Target Indonesia." Wired 18 Aug. 1998. 26 Jan. 1999 <http://www.wired.com/news/politics/story/14483.html>.

Godwin, William. Enquiry Concerning Political Justice. 1793. The Essential Works of Anarchy. Ed. Marshall S. Shatz. New York: Quadrangle, 1972. 5-41.

"Gulf War IRC Logs." 19:42, 16 Jan. 1992. IRC Chat. 20 May 1999 <ftp://sunsite.unc.edu/ pub/academic/communications/logs/Gulf-War/Jan-18-Scott>.

Guy, James J. People, Politics and Government: A Canadian Perspective. Scarborough, ON: Prentice-Hall, 1998.

Hager, Nicky. "Exposing the Global Surveillance System." Ham Radio Online 2 Feb.1998. 28 June 1999 <http://jya.com/echelon.htm>.

Harmon, Amy. "Hacktivists of All Persuasions Take Their Struggle to the Web." New York Times on the Web 31 Oct. 1998. 26 January, 1999 <http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+55538+0+wAAA+hacktivist>.

Harrington, James. "Beware of Chilling Freedom of Expression." CyberReader. Ed. Victor J. Vitanza. Needham Heights, Mass: Allyn & Bacon, 1996. 157-159.

Hermosillo, Paulina. "Interview: Bishop Samuel Ruiz García." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 71-72.

Hillis, Ken. "A Geography of the Eye: The Technologies of Virtual Reality." Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies. Ed. Rob Shields. Thousand Oaks, CA: Sage, 1996. 70-98.

Human Rights Watch (HRW). Human Rights Watch World Report 1998: Mexico. 1998. Dec. 1998 <http://www.hrw.org/hrw/worldreport/Americas-08.htm>.

Hundley, Richard O. and Robert H. Anderson. "Emerging Challenge: Security and Safety in Cyberspace." In Athena's Camp: Preparing for Conflict in the Information Age. Eds. John Arquilla and David Ronfelt. Santa Monica, CA: RAND Corporation, 1997. 231-251.

International Forum: Communication and Citizenship (IFCC) Home Page. May 1999. <http://quito.ecuanex.net.ec/foro_comunicacion/convocatoria_objetivos_eng.html>.

Josefsson, Dan. "An Interview with William Gibson." 23 Nov. 1994. 16 Jan. 1999 <http://www.algonet.se/~danj/gibson1.html>.

Kaplan, Carl. "For Their Civil Disobedience, the 'Sit-In' Is Virtual." The Cyberlaw Journal: New York Times on the Web 1 May 1998. 26 Jan. 1999 <http://www.nytimes.com/library/tech/98/05/cyber/cyberlaw/01law.html>.

Katzenberger, Elaine. "Living Conditions." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 33-34.

Krol, Ed. The Whole Internet Catalog & User's Guide. Sebastopol, CA: O'Reilly and Associates, 1992.

Kymlicka, Will. Contemporary Political Philosophy: An Introduction. New York: Oxford University Press, 1990.

Levy, Steven. "Cypher Wars." Wired Nov. 1994. Feb. 1999. <http://www.wired.com/wired/archive/2.11/cypher.wars_pr.html >.

Mandelbrot. "Resistance by Radio." Geist 8.34 (1999): 28-31.

Marcos [Subcomandante]. "Chiapas: The Southeast in Two Winds." Zapatistas! Documents of the New Mexican Revolution 1994. Dec. 1998 <gopher://lanic.utexas.edu/00/la/Mexico/Zapatistas/0>.

Martz, Laura. "Radio Free Yugoslavia." Wired 17 May 1999. 5 Nov. 1999 < http://www.wired.com/news/culture/0,1284,19715,00.html >.

Mathews, Jessica T. "Power Shift." Foreign Affairs 76.1 (1997): 50-66.

McKay, Niall. "Pentagon Deflects Web Assault." Wired 10 Sept. 1998. 26 Jan. 1999 <http://www.wired.com/news/news/politics/story/14931.html>.

McKay, Niall. "Hacktivists Join Activists." Wired 20 Nov. 1998. 25 Jan. 1999 <http://www.wired.com/news/news/politics/story/16401.html>.

McLaughlin, Margaret L., Kerry K. Osborne and Christine B. Smith. "Standards of Conduct on Usenet." Cybersociety: Computer-Mediated Communication and Community. Ed. Steven G. Jones. Thousand Oaks, CA: Sage, 1995.

Meeks, Brock and Declan McCullagh. "The Cyber Rights Report Card." Wired Oct. 1996. Feb.1999. <http://www.wired.com/wired/archive/4.10/cyber_rights_pr.html>.

Mohawk Nation News (MNN). "To Mohawks Going with Canada NAFTA Trade Mission to Mexico." 9 Jan. 1998. 12 Dec. 1998 <chiapas95@eco.utexas.edu>.

Nemeth, Evi, Garth Snyder, Scott Seebass and Trent R. Hein. Unix System Administration Handbook. Englewood Cliffs, NJ: Prentice Hall, 1995.

Nguyen, Dan Thu and Jon Alexander. "The Coming of Cyberspacetime and the End of Polity." Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies. Ed. Rob Shields. Thousand Oaks, CA: Sage, 1996. 99-124.

Novak, Marcos. "Liquid Architectures in Cyberspace." Cyberspace: First Steps. Ed. Michael Benedikt. Boston, MA: Massachusetts Institute of Technology, 1992. 225-254.

Nozick, Robert. Anarchy, State, and Utopia. New York: Basic Books, 1974.

Nye, Joseph. "Soft Power." Toward The Twenty-First Century: A Reader in World Politics. Eds. Glenn Hastedt and Kay Knickrehm. Englewood Cliffs, NJ: Prentice-Hall, 1994.

Paquin, Bob. "E-Guerillas in the Mist." The Ottawa Citizen 26 Oct. 1998. 26 Jan. 1999 <http://www.ottawacitizen.com/hightech/981026/1964496.html>.

Peltier, Leonard. "Statement of Support." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 139-155.

Peña, Guillermo G. "The Subcomandante of Performance." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 89-96.

Poniatowska, Elena, "Women, Mexico, and Chiapas." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 99-107.

Quittner, Joshua. "Free Speech for the Net." Time 24 June 1996. 10 Feb. 2000. <http://www.pathfinder.com/time/magazine/archive/1996/dom/960624/technology.html>

Rheingold, Howard. The Virtual Community: Homesteading on the Electronic Frontier. Reading, MA: Addison-Wesley, 1993.

Rochlin, Gene I. Trapped in the Net. Princeton, NJ: Princeton University, 1992.

Romano, Mike. "The Politics of Hacking." Spin Nov. 1999: 168-174.

Ronfelt, David and Armando Martinez. "A Comment on the Zapatista 'Netwar.'" In Athena's Camp: Preparing for Conflict in the Information Age. Eds. John Arquilla and David Ronfelt. Santa Monica, CA: RAND Corporation, 1997. 369-391.

Rosset, Peter. "Understanding Chiapas." First World Ha! Ha! Ha!: The Zapatista Challenge. Ed. Elaine Katzenberger. San Francisco, CA: City Lights, 1995. 157-167.

Ruffian, Oxblood. Interview with Blondy Wong. The Longer March. 15 July 1998. 24 Jan. 1999 <http://www.cultdeadcow.com/cDc_files/cDc-0356.txt>.

Rushkoff, Douglas. Cyberia: Life in the Trenches of Cyberspace. New York: Harper-Collins, 1995.

Schatz, Marshall. The Essential Works of Anarchism. New York: Quadrangle, 1972.

Schiller, Herbert I. "The Global Information Highway: Project for an Ungovernable World." Resisting the Virtual Life. Eds. James Brook and Iain A. Boal. Monroe, OR: City Lights, 1995. 17-33.

Shade, Leslie R. "Is there Free Speech on the Net? Censorship in the Global Information Infrastructure." Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies. Ed. Rob Shields. Thousand Oaks, CA: Sage, 1996. 11-32.

Shields, Rob. "Introduction: Virtual Spaces, Real Histories and Living Bodies." Cultures of the Internet: Virtual Spaces, Real Histories, Living Bodies. Ed. Rob Shields. Thousand Oaks, CA: Sage, 1996. 1-10.

Sterling, Bruce. "Internet." Fantasy and Science Fiction Feb. 1993. Oct. 1998 <http:// www.forthnet.gr/forthnet/isoc/short.history.of.internet>.

Sterling, Bruce. "So, People, we have a Fight on our Hands." Wired July 1994. Feb. 1999 < http://www.wired.com/wired/archive/2.07/sterling.cfp_pr.html>.

Sterling, Bruce. "The Hacker Crackdown: Law and Disorder on the Electronic Frontier." 1992. 12 Nov. 1999 <http://www.lysator.liu.se/etexts/hacker/digital1.html>.

Sun Tzu. The Art of War. n.d. Dec. 1998 <ftp://sunsite.unc.edu/pub/docs/books/ gutenberg/etext94/suntx10.txt>.

Szafranski, Richard. "Neocortical Warfare? The Acme of Skill." In Athena's Camp: Preparing for Conflict in the Information Age. Eds. John Arquilla and David Ronfelt. Santa Monica, CA: RAND Corporation, 1997. 395-416.

Thomas, Rebecca and Rik Farrow. Unix Administration guide for System V. Englewood Cliffs, NJ: Prentice Hall, 1989.

Toffler, Alvin. The Third Wave. New York: Morrow, 1980.

Von Clausewitz, Carl. On War. 1976. Princeton, NJ: Princeton University, 1989.

Wray, Stephen. "Electronic Disobedience and the World Wide Web of Hacktivism." 15 Oct. 1998. 26 Jan. 1999 < http://www.nyu.edu/projects/wray/HarvPresent.html>.

Wray, Stephen. "Worldwide Chiapas Protest Statistics: Version 2.2, Jan 14." 15 Jan. 1998. Dec. 1998 <chiapas95@eco.utexas.edu>.

Zapatista Army of Liberation. "Massacre in Acteal." Oct. 1998: <http://www.peak.org/~joshua/fzln/massacre.html>.

Zaferakis, Andrew. "Athena and Arachne." Pallas Athena. Nov. 1998. <http://www.clarkson.edu/~zaferaag/lf310/arachne.html>.