# THE SPATIAL DEMENTIA OF GEOPOLITICS: ONLINE AGENCY AND U.S. HEGEMONIC DECLINE

2002

IAN ALEXANDER OAS

The Pennsylvania State University

The Graduate School

Department of Geography

# THE SPATIAL DEMENTIA OF GEOPOLITICS:

# ONLINE AGENCY AND U.S. HEGEMONIC DECLINE

A Thesis in Geography

by

Ian Alexander Oas

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Master of Science

August 2002

# ABSTRACT

Cyberspace is a double-edged sword for United States hegemony.  The borderless world of cyberspace has facilitated massive capital accumulation and the extension of extra-territoriality for the United States.  However, cyberspace has subverted hegemonic power by providing innumerable political agencies portals into the U.S. – circumventing territorial borders.  Both economic success and political threats stemming from cyberspace on U.S. hegemony can be explained by using world-systems theory. Geohistorical analysis explains that hegemonies always promote the expansion of free trade through exporting a prime modernity and establishing extra-territorial institutions. This expansion leads to hegemonic decline, as other states become more adept at utilizing the technological innovations that had previously helped provide the hegemon an advantage.  The United States has pioneered the expansion of the capitalist world-economy into the virtual world – a network geography without territoriality – but in so doing, it has created a vacuum to be filled with political agencies other than the state.  By placing a qualitative study juxtaposing U.S. government policy on cyber-defense with the use of the Internet by online agencies in a geohistorical context, this thesis will explain why the United States increasingly finds itself the center of online conflict and from where attacks against it take root.  In turn, this will help answer the broader question of whether a new politics is forming based on a new network metageography and the implications this development has for U.S. hegemony and the capitalist world-system.

**Keywords:** United States hegemony, cyberspace, geopolitics, deterritorialization, political geography, world-systems theory

## Table of Contents

# Chapter One: Introduction

In addition to acting as a space for unbridled economic activity, the Internet is fast becoming an arena of political contestation and conflict. As the number of connections to this nodal network continues to expand indefinitely, cyberspace will increasingly become the medium of choice for political organization and mobilization. As the most “connected” nation-state in the world, and arguably the state most envied in the world-economy, it can be expected that much cyber-warfare will increasingly be directed against the United States and its political interests in particular. In the last several years, virtual attacks against the world hegemon have grown precipitously in number and effectiveness.

In 1998, the Pentagon registered just over 5,800 successful electronic break-ins via the Internet; in 2000, the number rose to well over 20,000. Attacks have become such a concern to the Department of Defense that the Pentagon has begun actively recruiting hackers to work for the government (Price, 2000). In the autumn of 2000, as Israel attacked Palestinians in the West Bank and Gaza, a Palestinian sympathizer broke into an American pro-Israeli lobby group’s web site and stole names and credit card numbers of its supporters (Schwartz, 2000). Many organizations based in the United States that support Israeli causes suffered website defacement and security intrusions. During the NATO campaign in Kosovo, Serbian sympathizers used the Internet to disrupt NATO military communications networks. With acts such as these foreshadowing the future of conflict, during his waning days in office former-President Clinton ordered the creation of a plan for military strategy in cyberspace (Messmer, 2000). In October of 2000, Michael Hayden, the head of the National Security Agency (NSA), noted: “Information is now a place. A place where we must ensure American security as surely as [in] … sea, air, and space” (CNN, 2000).

Hayden’s statement brings up an interesting paradox facing the world hegemon – cyberspace as a space for its extra-territorial dominance versus, in turn, the opening of its own territorial sovereign space to the vulnerability of network infiltration. Underlying

U.S. vulnerability to cyber-conflict is a Catch-22 of gaining economic advantage through the Internet, at the cost of giving up its own political sovereignty – that is, opening the floodgates to network intrusion. Perceiving the virtual world as a space or territory in which it needs to secure American sovereignty and national interests, the United States presumes that online political adversaries are territorially affiliated. However, this perception varies drastically from the reality of cyber-geography. As the most powerful political institution in the world-economy, the United States currently finds itself suffering from a form of spatial dementia – attempting to exert its geopolitical power over the network geography of the virtual world through territorial means. As will be shown, this has dire implications for the United States and global geopolitics in general.

## Problem Statement

Few can argue the fact that the Internet has been an economic panacea for the United States as hegemonic power. By expanding free trade into the virtual world and supplying a majority of the world's demand for computer technology, the 1990s saw U.S. corporations boost the hegemon out of lengthy recession and back into an economically dominant position (Baker, 1998; Heilemann, 2001). Upon critical inspection, however, in addition to being an economic asset, the Internet proves itself capable of undermining the U.S. hegemony that it currently helps maintain. This thesis focuses on how the Internet presumes the position of a double-edged sword, wielded by an aging knight, with the potential to dislodge the U.S. from its role of world hegemon.

The following pages and chapters of this study will contribute to research and begin addresing a much broader question – the role of territoriality in U.S. power. Facilitated by the movement of capital and financial markets to virtual space, the world economy has increasingly become structured as a nodal network. Under contemporary globalization, and fueled by networked telecommunications technologies, business has become increasingly transnational, muddying the traditional role of the state – to protect national economies (Hudson 2000; Sassen 1998a). Assuming that the nodal structure of the virtual world is, as will be discussed, ushering in a new metageography, this thesis examines how the political geography of cyberspace, as currently exemplified in the networks of the virtual world, impacts the geopolitical policies of the U.S.

Furthermore, the following project predicts what impingement networked political agency has, and will have, on the current world hegemony (Agnew, 1999; Taylor, 2000, 2001; Taylor, Beaverstock, & Smith, 2000). As will be concluded, the foundations of U.S. power lie not only in its position of global economic dominance, the technological savvy and size of its military, or simply in the cultural dominance of the U.S., but rather in what is a global complacency to a geopolitical order based on territoriality. As the Internet begins to undermine certain spatial restrictions on political agency stemming from territorial organization, the U.S. finds itself desperately needing to modernize itself to the realities of network conflict. Whether it will be able to do so is above and beyond this project; however, the following chapters will shed light on the processes behind the U.S. governments' attempts to modernize to the risks of the Internet.

## Theoretical Background

World-systems analysis will be used as the theoretical background to help answer the problems brought forth in this thesis. As will be discussed in detail in the second chapter, there are two reasons for my choosing this structuralist epistemology over others. First, world-systems theory is able to integrate economic, social, and political processes while looking at a number of geographic scales. An ability to observe trans-scalar processes is important when studying the Internet, as the political agents involved range from powerful nation-states to the most impoverished of individuals (e.g., Chiapas Indians of Mexico). Second, world-systems theory will be used to look at events in both a temporal and spatial context. Methods of geohistorical analysis help place the United States' current situation into a broader picture, with similarities and differences to past hegemonies proving most beneficial to analyze.

Yet, another profit of utilizing world-systems theory is that it proves particularly useful in the analysis of world hegemonies. World hegemony is defined as the economic leader in production, trade, and finance. However, as also will be discussed in Chapter

Two, much more than this, the world hegemon is a global leader, the state that maintains the geopolitical order and is envied by all other states. The world hegemon is able to forge consensus and coerce those outliers that refuse to acquiesce to its wishes through the power of its extra-territoriality. As will be discussed, hegemonic extra-territoriality, or the ability to push ones sovereignty and regulations across the borders of others, requires the development of institutions and technological innovations that help universalize one's ways (Taylor, 1996). As world leader, the world hegemony is often envied and identified as the epitome of modernity (Taylor, 1996, 1999). It thus becomes what everyone hopes to emulate, the prime modernity (Taylor, 1996). Since everyone desires to become like the prime modernity, they begin to mimic the world hegemon and consume from it. As will be shown, today the Internet acts as an innovation that helps the U.S. exert its hegemonic extra-territoriality worldwide through the incessant exportation of American culture twenty-four hours a day – the prime modernity of Americanization is continually spread across sovereign borders through the nodal network (Holloway & Valentine, 2001).

World-systems analysts and others specializing in geopolitics all concur that the United States is the contemporary world hegemon and has been since around the middle of the twentieth century (Agnew, 1993, 1998; Agnew & Corbridge, 1995; Arquilla & Ronfeldt, 1999a; Arrighi, 1994; Arrighi & Sliver, 1999; Brzezinski, 1998; Flint, 2001; Gibson, 2001; Gray, 1988; Keohane, 1984; Luttwak, 1992; Modelski, 1987; O'Tuathail, 1996; Taylor, 1992, 1993, 1996, 1999, 2001; Taylor & Flint, 2000; Wallerstein, 1987; Zakaria, 1998). Many argue that world hegemonies go through an identifiable cycle, generally lasting approximately 100 years (Agnew, 1993; Arrighi, 1994; Arrighi & Sliver, 1999; Flint, 2001; Modelski, 1987; Taylor, 1993, 1996, 2001; Taylor & Flint, 2000). In brief, as Chapter Two will discuss hegemony as defined by world-systems analysis, a hegemonic cycle begins with the hegemon's ascent to power and ends with its inevitable decline. Though many definitions of this cycle exist, it has been simplistically deconstructed by into four 25-year phases by Modelski (1987).[1] First, hegemony begins in the chaos of global warfare, during which there is a strong desire amongst states for order and stability, but due to equal footing and competition between various superpowers, stability remains unavailable (Modelski, 1987). After the dust settles, the second phase of hegemony begins with the state that has suffered least during the conflict rising from the ashes as the unparalleled world leader (Modelski, 1987). A strong desire in the inter-state system for geopolitical order remains, and through consensus building and military strength – the threat of which makes states fall in line – the hegemony becomes world leader and enforcer of the forthcoming period of stability (Modelski, 1987). During the third phase, however, states tire of the hegemon's yoke, and begin competing with the hegemon again. Distraught and tired of the hegemony's geopolitical world-order, states begin contesting certain aspects of hegemonic leadership (e.g., the French throughout history). As desire by states for the security provided by the current geopolitical order wanes, so does hegemonic ability to induce consensus (Modelski, 1987). In the fourth phase, inter-state competition and power seeking continually flares into global competition and warfare aimed at dethroning the hegemony. At this point, the stability a hegemony has maintained quickly dissipates (Modelski, 1987).

By most analytical accounts, including Modelski's own timeline, the United States is definitely in the third phase of delegitimization, if not already on its way into the fourth phase of ensuing competition and chaos (Agnew, 1993; Arrighi, 1994; Arrighi & Silver, 1999; Modelski, 1987; Taylor, 1993, 1996; Taylor & Flint, 2000). During the fourth phase, verbal and theoretical sparring with the hegemon often evolves into violent and overt methods of resistance. Potential cases of inflammation toward the U.S. geopolitical world order are ripe in the contemporary news media: September 11th, the EU announcing that it is supporting the PLO over U.S.-ally, Israel, and the Sino-Russian

[1] However, Modelski's breakdown is quite contentious. Many in the world-systems theory camp disown his model of the hegemonic cycle because it lacks a causal element. Whereas world-systems theorists believe that capital accumulation and economic factors drive the hegemonic cycle, Modelski argues that politics does. Thus, though roughly correlating with other world-systems theorists both temporally and theoretically, and though producing the easiest model to use in a generic capacity to descriptively describe the hegemonic cycle, Modelski's model will be used here only as an introduction to the process. It is not the driving theory or model behind this thesis, as will be discussed in Chapter Two.

military alliance against U.S. imperialism, et cetera. Yet, perhaps more tellingly than acts of international diplomacy, the U.S. and its allies increasingly find themselves at the center of virtual attacks far more frequently than other states (attrition.org, 2001). The Internet has become a prime medium for resistance against U.S. hegemony, and the use of virtual networks to attack the U.S. will only increase as the world becomes more interconnected (Arquilla & Ronfeldt, 1999a, 1999b, 2001; Cilluffo, Collins, Borchgrave, Goure, & Horowitz, 2000; Newman, 2000; Wray, 1998a, 1998b).

Of course, the U.S. is not a benign political institution. It will struggle to maintain its position of world hegemony, for better or worse, as long as it can. Though very contentious, Modelski (1987) has argued that hegemonies might be able to regain their position of dominance if they react and respond to the geopolitics of the fourth phase adeptly. In order to attempt such buoyancy in the midst of a changing metageography, however, the U.S. will need to modernize its internal mechanisms and institutions. If it fails to do so, there is a chance that other institutions will replace it.

This thesis will use Beck's theory on reflexive modernization and sub-politics in risk society to help illuminate U.S. cyber-defense policy decisions (1992). As will be discussed in Chapter Three, Beck (1992) argues that certain developments behind the evolution of modern society often have harbinger side effects, or "risks," that require new methods of political responsibility and regulation. Using nuclear weapons as his case study, Beck (1992) argues that nuclear capabilities were developed as an advantage to society, but due to their inherent capability to end life on the planet earth, they actually comprise a risk to even those responsible for their development. Thus, in risk society, from the development of perceived goods in modernity come unpredicted, and often uncontrollable, negatives. Due to new risks, and public outcry against them, state governments are often forced to adapt, or reflexively modernize, and create new institutions to regulate and alleviate the new menaces. As world hegemon, through its own prime modernity the U.S. has created numerous risks that it needs to reflexively modernize to in order to maintain its legitimacy as world leader.

As will also be discussed in Chapter Three, sub-politics – embryonic movements that forge around the risks of contemporary society – form when governments, or those in power, fail to reflexively modernize to risks (e.g., environmentalist movement against various governments). Sub-politics are not necessarily anti-systemic – wanting to change the capitalist world-economy – but they threaten the current institutions of political power and, sometimes, end up replacing institutions that refuse to modernize to new risks. Today, U.S. homeland defense is in the process of reflexive modernization, as it increasingly finds its actions based on territorial assumptions that neither exist in cyberspace nor, as terrorism is making more obvious, in the real world. Meanwhile, anti-systemic movements (political movements that are against certain features of the capitalist world-economy, such as globalization, patriarchy, environmentalist destruction, et cetera) are continually mobilizing, garnering support, and taking direct action against the U.S. and its institutions through the medium of cyberspace. Unlike sub-politics, which frequently evolve into new institutions of power, anti-systemic movements attempt to secure power through current institutions with the intent of using that power to change the capitalist world-system.

The network geography of cyberspace provides sub-politics and anti-hegemonic movements an unprecedented medium for asymmetrical warfare – the ability to attack strategic targets quickly and swiftly without the risk of direct retaliation. As will be shown, while the U.S. struggles to reflexively modernize to this new geography, its status as world hegemony continues to erode, and the powers associated with global leadership begin to wither. Thus, the invention of the Internet, which has given the U.S. an unprecedented avenue of extra-territorial power and influence across the economic and political borders of the world-economy, has begun to unfold back up on itself. The technological innovation and blessing of interconnected networked communications has begun to swing back as the unpredictable, and currently untamable, risk of the deterritorialization of political agency in the world-economy. As will be shown, the ability of the U.S. to create and implement effective policy, in the face of unimpeded anti-hegemonic dissent through the Internet, lies at the center of its ability to survive the transition from the territorial metageography of yesterday to the network metageography of tomorrow.

## Methodology

Geography is fundamental to better understanding the deterritorialization of global politics and the impact this is having on the United States' role in the capitalist world-system. Through analysis of the different spatial perspective held between the U.S. hegemon and non-state agencies operating online, systemic conflict between territorial and network political agencies can be better understood. This thesis embraces two methodologies to achieve the possibility of such analysis: archival research and electronic interviews (also referred to as electronic questionnaires). As this thesis's argument is based on research from actors of quite divergent backgrounds, both of these qualitative methodologies were chosen for their practical use in culling the necessary data from particular subjects – institutions affiliated with the making and shaping of U.S. cyber-defense policy, as well as online political agencies of various size and ideological background.

### Government Study

In order to gain insight into the U.S. government's policy decision-making and actions of implementation, an archival approach was used. The original thesis proposal, submitted September 15th, 2001, suggested interviewing government employees in various sectors of cyber law enforcement and policy making in order to gauge the direction of U.S. cyber-defense. However, after the events of September 11th, 2001, it became obvious that securing interviews with government agents would be difficult at best for the foreseeable future. Furthermore, certainty wavered over whether interviews would provide the most effective means to gathering data on the U.S. government spatial perspective. Interviews could only provide the individual opinions of particular bureaucrats and government employees, not necessarily the direction that U.S. defense policy is evolving (Lindsay, 1997; Silverman, 1993). Moreover, the number of people that needed to be interviewed to gain comprehensive insight on such policy making was daunting for a project as temporally limited as this one.  With other aspects of the thesis project having already commenced, a decision had to be made as to how best to gain insight on U.S. policy, without the originally planned interviews.

The RAND Corporation and the ANSER Corporation's Institute for Homeland Security are two of the leading policy-making think tanks influencing the Department of Defense's position on network security.  Both of these federally funded corporations produce a plethora of documents, studies, and analyses every year, providing data and suggestions to legislators and defense experts on Net warfare and defense against virtual attacks.  Thus, it was determined that through the comprehensive analysis of documents coming from these two corporations, as well as publications from groups affiliated with these corporations, U.S. policies and spatial disposition toward Net warfare could be comprehensively analyzed – arguably even more effectively than the originally proposed interviews.

Fortunately, the RAND Corporation is well recognized as a crucial component in the formation of U.S. legislation and strategy, and thus, many libraries around the U.S. house entire sections of RAND publications.  Paterno Library at the Pennsylvania State University (PSU) maintains a gargantuan section of such documents, including most of the recent publications pertaining to Net War and U.S. homeland defense.  Furthermore, RAND maintains a vast Website with many of their documents and most recent publications, which may have not yet found their way to Paterno Library, obtainable online.  As will be discussed in Chapter Four, the RAND Corporation is considered an unparalleled leader in policy shaping and making, and thus, archival research of their timely and easily accessible, though numerous, documents proved to be a most effective method of determining U.S. policy in cyberspace.

ANSER's Institute for Homeland Security is a relatively new policy making bureau, affiliated with, but quite independent from, the RAND Corporation.  Established in 2000, the Institute for Homeland Security publishes a journal, *The Journal of Homeland Security*, produces a weekly newsletter on homeland defense with a distribution of well over 10,000, and publishes documents and studies detailing homeland defense needs on a regular basis, much akin to the RAND Corporation. Through analysis of the Institute's journal articles pertaining to cyberspace – written by a wide-spectrum of defense experts, academics, and government officials, each offering their respective insight – a broad view of inter-agency conflict and congruence within the Federal Government was obtained. Furthermore, through review of pertinent newsletter links and news articles, analysis of current and past legislative efforts to enact policy decisions was possible. Whereas the RAND Corporation's documents detailed studies and potential directions for U.S. policy makers, ANSER's Institute for Homeland Security provided a periscope view into the inner workings of the forthcoming debate, fruition, and withering of these various policy recommendations.

Through archival research of upwards of 25 published documents from the RAND and ANSER corporations – many of which have often been referred to by various policy experts and Congressional circles as important and prime documents in understanding the United State's position on cyber-defense – a thorough investigation of U.S. spatial perspective in the face of deterritorialized conflict was derivable. Standard methods of keyword searching and document coding were used in the analysis (Crang, 1997; Creswell, 1998). In conjunction with these documents, numerous shorter pieces and reports on Congressional and Presidential positions on such policy recommendations, obtained through the Institute for Homeland Security's weekly newsletter, provided the research with guidance as to what studies were most pertinent to actual U.S. decision-making. They also helped contextualize the documents within the inter-agency debates over policy changes at the Federal level (Elwood & Martin, 2000; Oberhauser, 1997). In the end, archival research proved, not only worthy for this study but, far more thorough than the originally proposed interviews.

### Online Agencies: Hackers, Crackers, and Radicals, Oh My!

The methodological approach used to study non-state political agency in cyberspace was that of the case study. Creswell notes that "instrumental" case studies focus on a particular issue and use their samples to illustrate this (Creswell, 1998, p. 62). The issue in this study is the extension of political agency into the nodal network of the Internet and its role in fighting, either overtly or inadvertently, U.S. hegemonic power and interests. This study uses a “holistic analysis” (Creswell, 1998, p. 63) of all online cases to better illustrate the impact of online political agency in the geopolitical world order. Though primarily basing its analysis on interviews, as Creswell argues, a good case study should embrace more than one method of data collection (1998, p. 63), and thus research of other interviews with similar cases (e.g., hackers), the background of non-state agency in cyberspace, and direct online observations were incorporated as well. Through careful analysis of the data, including the interviews and background research, and by placing analysis in the temporal context of declining hegemony, the researcher was able to make certain assertions about the political and spatial philosophies and meanings of contemporary online political agency.

Though a phenomenological approach may have worked for data collection as well, due to the temporal constraints of a obtaining a Masters thesis the case study was the most realistic approach. Furthermore, though the researcher has some background in cyber-subterfuge, he is incapable of sharing an experience with his subjects as phenomenology often demands (Creswell, 1998, p. 51-55). Creswell argues that phenomenological studies often bring a “philosophical perspective” or “orienting framework” that “informs what will be studied and how it will be studied” (1998, p. 86). Creswell believes that proper analysis of data through this framework might provide a “description of the ‘essence’ of the experience” – in this case, the experience of using the Internet politically against the state (Creswell, 1998, p. 65). However, for the scope of this study, a phenomenological method might have diverged off tangent from the problem statement – becoming more focused on the essence of agency than the geography of deterritorialized conflict. Furthermore, the political sciences rarely embrace phenomenology (Creswell, 1998, p. 65), and this thesis makes use of numerous political theories. Thus, it was decided to conduct a case study of various agencies operating online and avoid a potential methodological-theoretical divide.

Creswell (1998) argues that case studies should maintain a limited amount of samples, or cases, so as to not water down the research. Intense analysis of samples is preferred over a large quantity of samples (Creswell, 1998). It was with this argument in mind that the cases for this study were chosen. In the end, four large organizations and six self-described “hackers” and “crackers” were analyzed from the milieu of political agencies online. These cases were selected based on two criteria: first, their willingness to answer a long questionnaire and subject themselves to follow up questioning, and second, their role in online politics and agency.

The sheer size and magnitude of the Internet make the logistics of conducting a study on virtual politics quite daunting. With hundreds of millions of users online around the world, any case study of participants in the virtual world must note that its sample is not definitively thorough. On top of providing a headache to territorial institutions of power, the geography of the Internet also induces various problems for those attempting to embrace conventional techniques of scientific data acquisition. Figuring out proper sampling methods and sizes is inherently difficult in an ephemeral, non-territorial landscape. The quantity of potential samples is incalculable, and traditional measurement of distances between samples is impossible in the ephemeral geography of the networked virtual world. Such dilemmas definitely posed a problem for deciding how many cases to study. Creswell (1998, p. 62) notes that in case studies “purposeful sampling” is often the best approach – “select[ing] cases that show different perspectives on the problem, process or event” being studied, in conjunction with random and ordinary cases. The online organizations interviewed in this study represent purposeful sampling – chosen for their backgrounds that all illustrate different aspects of online agency, sub-politics, and anti-systemic ideology. These cases were used in conjunction with randomly selected hacker interviews.

Initially, access to online political agents proved more difficult than envisioned in the project proposal. Not only are hackers and online political groups often loath to trust virtual personas asking them questions about their methods and philosophies, due to their strong cyber-disposition, they are nearly impossible to contact via traditional means in the real world. Traditional methods of conducting interviews were never a true option with online cases, as a primary reason for networked individuals' online abilities is the anonymity afforded them from the physical world (Elwood & Martin, 2000) – e.g., the nineteen-year old neighbor down the street being the cracker to bring down a bank in Singapore. With online interviews the only truly viable method, two hurdles remained to collecting data: human subjects approval for interviewing random, unidentifiable subjects, and finding random, unidentifiable subjects that were willing to conduct such interviews with an unidentifiable interviewer.

The hacker cases were randomly approached. These denizens of the Net were easily accessible in chatrooms, often openly exchanging information on hacking tools, stolen credit card numbers, and boasting about break-ins. In the midst of this, the researcher sent out an open invitation to all the people in the hacker lounges explaining that he was conducting interviews for a Masters thesis studying politics in cyberspace. When persons would answer, they were sent an implied consent form via private messenger. The interview commenced shortly thereafter.[2]

Organizations functioning online were found and selected on a different set of criteria from the hackers. Numerous political organizations were solicited for the study, but unfortunately, many never responded to the initial inquiries and others, after showing interest, never replied with answers to the questionnaire. In the end, only four organizations responded with enough clamor to be considered for the study, but fortunately, these four organizations were the primary ones sought in the purposeful sampling (Creswell, 1998, p. 62) by the researcher, and thus, they brought to the study a diverse set of political agendas and ideologies. Therefore, though the number of responses from these groups was less than hoped for, the answers obtained from the diverse organizations that did reply – from feminist fronts to Communists – were very comprehensive, informative, and often contained more useful information than had been anticipated.

[2] A small pilot study was conducted in December 2001. Questions were asked of several hackers, and though the data were useful, the transcriptions were eventually thrown out. From analysis of their answers, irrelevant questions were dropped from future interviews and some questions, which were deemed leading or poorly worded, were subsequently altered for the better.

Due to the anonymity promised in the consent forms accompanying the questionnaires, all of the online organizations have been given pseudonyms.  The first one, which will be named the *Socialist Front* (SF), is an international political party that views itself as "a worldwide movement against globalization" and that maintains a stance that is, obviously, "pro-Socialism."  It operates on a local and statewide basis, but is an interconnected global movement, and as will be discussed in Chapter Five, uses the Internet to help achieve global organization and mobilization.

The second movement analyzed is a large feminist organization that will be called the *Feminist Confederation* (FC).  Its origins are in the United States, but it partakes in international issues and has affiliations around the globe.  As will be seen, this organization is very proactive in international politics concerning women's rights around the world, as well as in protesting against U.S. government policy and laws that it views as hurtful to women.

The third case organization is an international environmental movement with offices around the world.  Hereon referred to as the *Green Earth Movement* (GEM), this organization mobilizes against state and international policies that are "environmentally disastrous" or that hold serious implications for the "Earth's ecosystems."  The GEM is very active politically in the real world, but in recent years has shown a marked increase in the use of network technology and online protest.

The final online group studied, is a non-profit organization with corporate sponsors.  This case diverges quite significantly from the others, as it does not view itself as political – not fighting for a cause per se – yet as will be shown, its actions are inherently political.  Concerned with helping other nonprofit organizations better utilize the Internet to bolster their funding and enrollment, *Non-Profit Net*'s (NPN) "mission is to achieve the Internet multiplier effect and make more nonprofits more important in more people's lives."  Though NPN does "not use the Internet for protest," they feel "the Internet multiplies social and philanthropic efforts to build a better society" and that "it is very effective in facilitating a method for many to speak out on issues they care about."

The study used email questionnaires, or interviews, to cull data from the organization and those interviewed in the chatrooms. This method was decided upon for two reasons. First, email interviews have been used and perfected as a method in the discipline of journalism for years (Wright, 2001). Though a relatively new concept to the social sciences, Dillman details methods of online data collection in his work, *Mail and Internet Surveys* (2000). In this breakthrough publication, he analyzes how best to utilize email interviews and acquire information over the Internet in a concise and direct fashion (Dillman, 2000). Online interviews and questionnaires have been praised for their potential, if done well, to be less subjective, less likely to be contaminated by the researcher, and for allowing the interviewee the time and solitary comfort to respond carefully to all pertinent questions (Dillman, 2000; Wright, 2001). Furthermore, by interviewing online, many issues of power relations between the interviewer and interviewees were avoided (Elwood & Martin, 2000), as the place of the interview was virtual and, arguably, more neutral. The questions were intentionally left open-ended, as in a case study it is important to allow the respondent to provide data without outside impediments on length and syntax (Oppenheim, 1992, p. 94-95). The email questionnaires allowed subjects to more easily ignore uncomfortable or unanswerable questions as compared to in-person interviews – where a respondent may feel compelled to respond (Wright, 2001). However, it must be noted that one downside to electronic interviewing is that it diminishes the ability of the researcher to engage in direct participant observation during the interview, which many texts on methodology opine is of help in analysis (Creswell, 1998; Elwood & Martin, 2000; Lindsay, 1997, p. 35-69; Oberhauser, 1997; Silverman, 1993).

In contrast to what is lost in online interviewing, the second reason email interviews were used in this project was that they are less threatening, and far less intrusive, than traditional methods of interviewing – easily discarded by the interviewee if so desired (Dillman, 2000). Simply by hitting the delete key, any wavering or noncommittal case is free of all hassle and intimidation. Meanwhile, such interview and survey rejections hold little financial burden to the study – unlike postal surveys (Salant

& Dillman, 1994) – when they remain unanswered (Dillman, 2000). Overall, the email questionnaires proved a stunning success, with respondents either typing their answers right into the electronic documents and returning them via email, or as in one case, someone recording their answers audibly and uploading them online for the researcher to download later.

The ORC approved interviewing hackers in chatrooms online under the condition that the interviewees were given an implied consent form, which illustrated the dangers of answering questions in cyberspace – i.e., one's answers supposedly run a "risk" of being intercepted by unidentified third parties.[3] Though hampering interview efforts – few individuals enjoy reading a three-page document delivered via instant messenger (see Appendix I) – in the end the consent form thwarted fewer interview attempts than originally envisioned by the interviewer. It is estimated that approximately seven interviews ended upon displaying the consent form mentioning potential risk of interception and possible court subpoena.

After scouring online chatrooms pertaining to hacking and hacktivism, research was primarily conducted in the relatively safe confines of Yahoo!Chat.[4] Limitation of interviews to this location was decided upon for several reasons, many of which stem from Elwood and Martin's (2000) piece on placing interviews. First, the interviewer's network security was a concern. Many chat programs have well known, and as it turns out frequently discussed, security flaws in them that allow knowledgeable individuals to raid another's computer while chatting. After initial research began for this project, the company that makes the Instant Relay Chat (IRC) program – arguably the most widely

[3] Ironically, the fact that the ORC made the interviewees' consent form mention threat of "third party interception" of answers in cyberspace only strengthens this thesis's final argument. New policies aimed at reflexive modernization, and made with every intention of bolstering security in cyberspace, are often seriously flawed and may actually stymie the benefits of using the Internet. For example, if this study had necessitated conducting a telephone interview instead of an "electronic" one, the consent form would have made no mention of the threat of interception of the telephone call by third parties, even though such interception is far easier, and far more rampant, than intercepting packets of digital information (TCPs) and piecing them together in cyberspace – a trick which, to this day, still has never been perfected. Comfort level with the technology of the telephone, which upon its original creation was deemed a risk to society at large much as the Internet is today (Martin, 1998), has grown to the point of indifference; whereas, cyberspace is still perceived as a greater potential risk in many ways – often irrationally.

[4] Available to anyone with Web access for free at: http://chat.yahoo.com.

used chat program in the world – announced that it had known about such an exploitable security glitch in its software for sometime before providing a patch to fix the problem. In contrast, Yahoo! has fairly stringent chatroom rules and a secure chat program that, if anything, errs on the side of security – frequently booting users off accidentally.

The second reason for deciding upon Yahoo!Chat was due to the variety of hackers found in Yahoo!'s three "hacker lounges." Observing call names for several weeks before actually conducting any interviews, it was apparent that though regulars frequented the rooms at varying schedules, overall there was a wide range of different users – hundreds, if not thousands, of different chatters in the 20-odd hours I spent observing before soliciiting interviews. At any one time there are approximately seventy chatters in the hacker lounges, often answering questions about how to crack into AOL accounts, steal programs off the Internet, and frequently challenging one another to attempt to break into each other's networks.

The interviews in the chatrooms varied in length, strength, and even medium. Some hackers were paranoid of instant messaging, as it is easily recorded. Since they could not be certain of who I was, they would make me ask questions in the generic chatroom, where their answers were not directly linkable to my questions – separated by lines of other chatters' jabberwocky. Yet, others refused to answer my questions in the chatroom itself, and only through private, or instant-, messaging would they accept the questions. These people often feared that by answering my questions in the main room, other hackers might suspect them of conspiring with a government agent, a corporate spy, or for that matter, even a lowly academic. The cases were allowed to determine where in the chatroom they would like to be interviewed in order to relinquish some of the power processes taking place between interviewee and interviewer (Elwood & Martin, 2000).

Conspiracy ladled and extremely suspicious minds aside, over time and after much observation into the culture of hacker speak, interviews with hackers were easier to obtain than initially envisioned. Much of their comfort in participating may have been due to the interview's location (Elwood & Martin, 2000) – in cyberspace, a space far more comfortable to them than it is to a graduate student in geography. As will be discussed in chapter five, some hackers were extremely conscious of the political agency in their actions, whereas others were confused by the prospect that their hobby had any political impact whatsoever. The answers to the questionnaire were varied, but similar themes ran throughout most of them. In general, the interview questions came straight from the IRC approved form (see Appendix II); though, the researcher would often use follow-up questions to illicit more explicit replies and guide the interviews further along previously unforeseen, but relevant, tangents – albeit this was done carefully so as to not lead the answering (Oppenheim, 1992).

The interview and questionnaire data were coded into themes consistent with this thesis's research agenda and established qualitative methods (Crang, 1997; Creswell, 1998). In the end, twelve meta-codings presented themselves: territoriality; network; politics; purpose; scale; spatiality; communication; organization; mobilization; economics; methods of Internet use; and regulation. These were created from numerous sub-codings – e.g., regulatory concern; future of hacktivism; anarchy; control; government; history; hacking; information diffusion, et cetera.

## Qualifications

Though pleased with the results of this project's methodologies, at this point several qualifications and answers to particular research problems should be asserted. The first and most glaringly obvious issue is whether the sampling technique chosen for hackers and online organizations was the best one. In essence, a question of how many interviews are enough needs to be addressed. Along the same line of thought, another area of potential contention lies in the process of selection. Were the methods used to of find online organizations and hackers objective?

Depending on the looseness of semantics, there are arguably millions of "hackers" in the world. It has been argued that in reality only about 1,000 are "elite" (Sterling, 1993) – capable of actually breaking into defense computers and knocking satellites out of orbit – while others espouse that there are potentially thousands that might implement such carnage (Anonymous, 2000; Hacktivist.com, 2001; Hafner & Markoff, 1995;

LoBaido, 1999; Price, 2000; Swartz, 2001; Wray, 1998a). Due to their lack of territoriality and their penchant to come and go in the chatrooms ephemerally, systemic sampling – that is "select[ing] with numerical or spatial regularity" (Earickson & Harlin, 1994, p. 44) – was not an option. Stratified sampling proved impossible as well, due to the number of individuals coming and leaving the chatrooms. Thus, random sampling of hackers, from which qualitative answers could be coded and a collage of ideas and beliefs analyzed, proved to be the most realistic approach. Though risk of a too narrowly focused and biased perspective was an initial concern, enough interviews were obtained for particular transcendental spatial and political themes to become apparent – which was discovered in the coding. These themes are the ones discussed in Chapter Five, with other less concentrated views blended in to show variation and dissent in the subjects' perspectives.

As for the objectivity of my organization sampling, online organizations were selected via Internet search tools – primarily Google.com. Upon hearing about an organization through either the Hacktivist Website, or other online sources, I would find the organization and email it asking for an interview with someone knowledgeable of its online activities.[5] Selection of potential case organization was broad, with a wide variety of political affiliations represented, including corporate backed non-profits, international political parties, environmental movements, and feminist fronts. Unable to control those who responded, versus those who failed to, the selection was still varied enough to provide insight as to how these organizations utilize and spatialize cyberspace in a political capacity. In some cases, follow up questions were sent to organizations in order to gain more information, and articulation, on their original answers.

## Conclusion

The network geography of cyberspace is deterritorializing international politics, and thus, cyberspace is a mixed blessing for a U.S. hegemony in decline. However, the U.S. is attempting to reflexively modernize to the new risks stemming from a deterritorialized

[5] The Hacktivist Website is available at to everyone with Web access at: http://www.thehacktivist.com.

geopolitical landscape and a potential new network metageography. Meanwhile, anti-systemic movements, those against U.S. hegemony and the capitalist world-system, as well as sub-politics, those attempting to forge new institutions to control the “risks” and opportunities of cyberspace, are using the cyber medium to organize, mobilize, and asymmetrically confront the U.S. and its institutions. This conflict between the world hegemony and a plethora of non-state actors is really the result of a battle between two political geographies – network organization versus territorial, hierarchical structure.

Through the juxtaposition of U.S. policy projects with the philosophical underpinnings and actions of non-state actors operating online, the implications of a metageographic shift on U.S. hegemony can be clearly outlined. In the following chapter, an overview of world-systems theory and the hegemonic cycle within the capitalist world-economy will be provdided – with special emphasis on the U.S. This chapter will include discussions on hegemonic extra-territoriality, the role nation-states maintain in the world-economy, and an overview of concepts of sovereignty. Chapter Three will illustrate theories of metageographies and metageographic shifts, provide a historical overview of the Internet and its economic benefits to the U.S., review the birth of online political agency, philosophies behind online agency, and review concepts and analyses of Net War. Chapter Four will dive into the analysis of the U.S. perspective on cyber-defense and the security risks associated with cyberspace, discussing policy recommendations and the ensuing spatial dementia of U.S. decision-making. Chapter Five will analyze online political agents and the spatial perspectives harnessed by agencies operating in and using the Internet as an economic and political tool against the hegemonic geopolitical order based on sovereign borders and territorial regulation. Chapter Six will tie the themes of all the previous chapters together, offering a conclusion to the problem statement: how does the deterritorialization of political agency affect U.S. hegemony and what are the geopolitical implications.

# Chapter Two: World-Systems Theory and Hegemony

The Internet acts as a double-edged sword for United States world hegemony. In addition to being an economic tool promoting hegemonic extra-territoriality, the Net has the political and spatial potential to *undermine* continued United States hegemony. It may appear ironic that as hegemonic power the United States has overseen and facilitated the expansion of the Internet to the point of disenfranchising itself as the most powerful state. However, geohistorical analysis demonstrates that technological innovation and capitalist expansion are commonly found to sabotage hegemony. Due to the vast array of components going into the assertion that cyberspace holds serious implications for continued U.S. hegemony, a theoretical foundation for this argument needs to be inclusive of three components: 1) a holistic interpretation of economic, social, and political processes; 2) the ability to incorporate all political agencies; and 3) the opportunity to place events in both a temporal and spatial context. World-systems theory provides all three of these elements.

This chapter will review the body of world-systems literature concerning hegemony as a cyclical process. After first providing an overview of world-systems theory, hegemony will be thoroughly analyzed, paying particular attention to the dynamics behind hegemonic ascension and subsequent decline. This topic will carry into a discussion of modernity, extra-territoriality, and sovereignty, and these concepts' application and influence in fostering hegemonic power. I will tie the chapter together with a discussion of anti-systemic movements and the implication they hold for U.S. hegemony, which will carry over into Chapter Three.

## World-Systems Theory

The primary goal of world-systems theory (WST) since its inception into the social sciences has been to provide a trans-disciplinary and holistic approach to the analysis of economic, social, and political processes within the world-economy. In order to achieve this objective, the theory's originator, Immanuel Wallerstein, needed an overarching system that incorporated all human activity – something missing in state-centric approaches such as Marxism (Taylor, 1987). Wallerstein found the system he needed in the *capitalist world-economy*. Within the WST framework, one can analyze economic, social, and political processes through both space and time. The capitalist world-economy can be broken down into three components: a single world market, a multiple-state system, and a three-tier structure (Taylor and Flint 2000, p. 18-33).

### Single World-Market

World-systems theory is based on the belief that there is currently one world-economy – an expansive economic system – that lacks a partner political system and must be analyzed as a single, unified structure (Parker, 2001; Taylor, 1981; Taylor & Flint, 2000). Commodity prices are determined by the world-market. Since these prices are not fixed, producers constantly compete for advantageous economic exchanges (Taylor & Flint 2000, p. 19-21). Political interactions within the world-economy are stimulated via competition to ceaselessly accumulate capital. Due to this competition, the world market ends up determining the location of various types of production, which in turn results in uneven development (Taylor & Flint 2000, p. 19).

Though world-economies are believed to be transitory, fueled by the ceaseless accumulation of capital, historical capitalism has been the world-economy since the 1600s (Parker, 2001; Taylor & Flint, 2000). The capitalist world-system originated in Europe, initially forming under Dutch hegemony. By the twentieth century the system had expanded to encompass the entire world. Different types of historical systems existed before the capitalist world-economy; however, capitalism is the first system to encompass all of humanity.

### Three Tier Structure: Political Processes and Scale

Expanding on Marx's core and periphery argument, Wallerstein divides power into three types of economic processes (Parker, 2001; Taylor & Flint, 2000): core (the exploiters), semi-peripheral (both exploiters and exploited), and peripheral (the exploited). It is important to note that core and periphery represent processes, not territorially fixed areas (Flint, 2000). Core processes are those that exploit for political and economic gain. Peripheral processes are those that result from exploitation. Areas such as states are referred to as core or periphery based on which process dominates in the given demarcated area; however, in core states you will find peripheral processes (e.g., homeless people begging outside the White House) and in peripheral states core processes (e.g., Noriega dealing cocaine from the Presidential Palace). Through these processes, world-systems theory provides a framework in which to analyze the movement and dynamics of power conflicts within the capitalist world-economy.

In the early 1980s, Peter Taylor began adapting world-systems theory to political geography by devising three interconnected scales through which power processes work (Taylor, 1981, 1987). First, there is the local scale, which he calls the “scale of experience” (Taylor, 1987, 2001). It is here where people experience their lives, in a local setting. Next up the ladder, the nation-state scale acts as a filter between the local and global scales. Taylor calls the nation-state the “scale of ideology,” as it is at this scale that social perceptions of the world are forged by class and national processes (Taylor, 1987, 2001). Finally, the “scale of reality” is that of the entire capitalist world-economy operating above and beyond the state. This scale is the one already referred to several paragraphs ago – the all-encompassing scale in which human agency takes place (Taylor, 1987, 2001). These scales provide a vertical geographic spectrum to the capitalist world-system and facilitate the geohistorical analysis of political processes (core and peripheral) operating through all levels of the world-economy.

Taylor’s theory has guided much of the research on scale over the past 20 years, but recently it has been at the center of criticism. Marston (2000) argues that Taylor’s work on scale in WST is too centered on the relations of capital production. Though she sees nothing inherently wrong with this approach, she feels it is exclusive and narrow in its scope of analysis (Marston, 2000). She argues that other processes factor into this production, including patriarchy and the gendering of social relations (Marston, 2000). As will be discussed later in this chapter, due to its inherently structuralist epistemology, many critique Taylor’s version of world-systems theory as being functionalist (Harvey, 1987; Skocpol, 1977). However, throughout the discipline, Taylor’s theory is now accepted as a relevant framework within which to analyze economic and political processes (Marston, 2000).

## Multi-State System and Institutions of Power

Though not focusing on the state scale, the multi-state system of political entities based on territorial demarcation is an *intrinsic* and *necessary* component of the capitalist world-economy. Without numerous states, the world-economy would not exist and instead, under the domination of one political authority, the system would be a world-empire (Taylor & Flint 2000, p. 11).

*States* represent the dominant institution of political power in the world-economy. Stemming from competition in the world-market, states have been constructed as both defensive and offensive mechanisms that “can distort the market” in the interest of core power processes operating within a given territory (Taylor & Flint 2000, p. 11). Thus, elites can use the state to protect their production interests from elites elsewhere. Furthermore, elites can use strong states to alter the world-market beyond their sovereign borders, providing economic advantage through the peripheralization of other states (Taylor & Flint 2000, p. 11). These competitive processes between core and peripheral state institutions result in an ongoing struggle for power and position within the world-economy.

Political power in the world-economy does not manifest itself in states alone, however. In fact, as already mentioned, WST varies from other theories in that it believes state-centric discourse is self-defeating. Though states comprise the primary institution of power, other institutions form to facilitate “the extraction of economic surplus for accumulation within the world-economy” either via market processes or through the use of political power (Taylor & Flint 2000, p. 25). In addition to the state there are *three* political institutions of importance to WST: households, peoples, and classes.

Households are one of the smallest political institutions in the world-economy. They allow the pooling of multiple incomes, and are maintained through the reproduction cycle as a viable political institution beyond the life of a human (Taylor & Flint, 2000, p. 27). Even within the household core-periphery processes are at work. It is in the institution of the household that the most primitive form of power is often practiced with no exogenous consequence – physical and mental violence (Taylor & Flint 2000, p. 28) – and from here that patriarchal relations permeate all types of power processes in the world-economy.

Institutions of *people* exist due to the diversity of personal existences varying around the world and throughout humanity. However, categories of people are often socially constructed to legitimate the peripheralization of the many for the economic benefit of the few. These institutions are fundamentally key for legitimizing wealth disparities and for mobilizing political resistance. Two prime examples of constructed peoples are *race* and *nation* (Taylor & Flint 2000, p. 28-30). Race is a product stemming from imperialist expansion of the capitalist world-system; the European core classified people on the basis of skin color to legitimate the peripheralization of non-European, persons (Taylor & Flint, 2000, p. 28). The construction of the nation as a political institution originates from state attempts to justify the maintenance of numerous political sovereigns, including wealth disparities between them (Taylor & Flint 2000, p. 29). The institution of the nation is often used to unite people to a territory.

Finally, as WST is a neo-Marxist theory, class is definitely heralded as a prime political institution of the world-economy. Though congruent with traditional Marxism in viewing class conflict as central to any theory of power, there are fundamental differences in how WST defines the class strata, e.g., labor is defined as those who directly produce a commodity – waged or not (Taylor & Flint 2000, p. 30-31). Furthermore, *controllers of production* are not necessarily the *owners of production* as Marx defined them (Taylor & Flint 2000, p. 30-31). Though important as a political institution, class does not necessarily entail ownership or wages, as it does in the Marxist sense, and it is constructed through core-peripheral processes.

This perspective of production and ownership does not sit well with all structuralist geographers, and marks a cataclysmic break in theory with the standard Marxist approach. In particular, David Harvey has been critical of world-systems theory and, particularly, Peter Taylor's adaptation of it for geographic purposes. Harvey disagrees with Wallerstein over the designation of the controllers as owners of production, accusing Wallerstein of misinterpreting "market exchange" with the ordinary circulation of capital (Harvey, 1987). Harvey believes that the "capitalist world-economy," around which world-systems theory is based, is in actuality no more than the misidentified "world market" (Harvey, 1987). Taylor, however, retorts that viewing national economies as independent entities within a world market is a fatal error in Marxist theory, not world-systems (Taylor, 1987). States actually operate within a world-system at the global scale.

Of the four above political institutions, the state is the most heavily analyzed due to its ability to manifest more power than other political institutions. Political conflict in the world-system is often based around scale, with those in power always attempting to contain the conflict to a scale falling within their political control, and those without power always attempting to expand the scale, or scope, of conflict beyond their adversaries' control (Schattschneider, 1960). The state's function within the scale of the reality (operating at the world-economy level) naturally places it in a position of institutional dominance. As the institution of the state is embedded within capitalism, it becomes imperative to review the economic growth cycle of the world-economy, and thus, the dynamics fueling state transitions and geopolitical power struggles – the Kondratieff Cycle.

## Dynamics of the Capitalist World-System

The capitalist world-economy develops in a cyclical pattern (Taylor & Flint, 2000). Nikolai Kondratieff was the first to argue that economic patterns, lasting approximately 50 years each, are crucial to the development of the world-economy. Kondratieff cycles consist of two epochs: the *A-phase* and the *B-phase* (Taylor & Flint, 2000, p. 14-17). The

A-phase is identifiable by 25 years of steady economic growth.  It is followed by the B-phase – approximately 25 years of economic stagnation and restructuring.  There have been four cycles – eight phases – since the beginning of the capitalist world-economy in the 17th Century.  Since Kondratieff's observation, world-systems theorists have embraced his cycles as adequately illustrating how the capitalist world-economy continues to grow and expand (Taylor & Flint, 2000, p. 14-17).  In addition to the structure of the world-economy, the economy's temporal dynamics (as represented by Kondratieff cycles) offer a geohistorical matrix for describing political processes (Taylor & Flint, 2000, p. 17).  Quite simply, these temporally contingent waves are important "because they help to generate cycles of political behavior" (Taylor & Flint, 2000, p. 17).

A-phases represent episodes of global overproduction.  As Taylor and Flint note, Kondratieff waves "are certainly associated with technological change, and the A-phases can be easily related to major periods of the adoption of technological innovations" (2000, p. 14).  A geohistorical gaze illustrates that the A-phases of all Kondratieff cycles coincide with major technological breakthroughs that drastically reshape the world.  During A-phases, producers attempt to collect as much capital as possible through the production of, and profits from, new types of technology (Taylor & Flint, 2000, p. 15-16).  This overproduction, though logical for individual producers at the time, fails to work for the system as a whole, and eventually, the ensuing gluttony of commodities leads to economic stagnation.

The B-phase occurs when overproduction in the preceding A-phase leads to a period of systemic reconfiguration (Taylor & Flint, 2000, p. 16).  The B-phase of Kondratieff waves is necessary to regenerate conditions for economic expansion and overproduction.  During B-phases the cutting-edge technology of the preceding A-phase is diffused to peripheral states, as core states begin to toy with newer "state-of-the-art" technologies (Taylor & Flint, 2000, p. 16).  Thus, processes of production previously associated with the core shift to the periphery and core states compete to become dominant in new areas of production and economic technology.

It is this period of technological replacement that often erupts in political struggles evoking state attempts to secure core processes within their territorial sovereign (Taylor & Flint, 2000, p. 16-17). Though overly simplistic, Agnew and Corbridge make an analogy of the struggle over power in the world-economy to those fighting over a pool of water – the amount of water is fixed, and therefore, one's gain must result in another's loss (Agnew, 1998; Agnew & Corbridge, 1995, p. 131). Perhaps a better analogy, however, might be that institutions fight for the clean water in this pool, and the losers, or peripheralized, are left with nothing but the sludgy remains. Not all states can gain equal access to economic power, for the result would be an end to core-peripheral processes (Agnew, 1998). Thus, each B-phase sees some states secure more core processes within their borders at the expense of others. Perhaps more importantly, however, the B-phase generally sees the expansion of the world-economy to yet more populations and territories, peripheralizing them, and therefore increasing the pool of power to those core states already in the fold. Though methods vary, each B-phase expands the world-economy to facilitate gains in power. The key is that all states, as institutions in the world economy, attempt to gain core processes within their sovereign territory. The catch is that since the entire globe has been in the capitalist world-economy since the beginning of the twentieth century, those who are peripheralized find themselves increasingly burdened by those in the core who accumulate more capital (Agnew & Corbridge, 1995, p. 131).

Beyond recognizing core-peripheral production realignment, Kondratieff cycles also facilitate the temporal demarcation of geopolitical orders. Paired Kondratieff cycles, two A-phases and two B-phases, roughly correlate with the rise and decline of world hegemonies (Taylor & Flint, 2000, p. 69-74). As will be thoroughly discussed, world hegemonies represent the dominant state institution of the world-economy, and are a crucial component to the world-system's continued expansion and vitality. The past two hegemonies, Great Britain and the U.S., have been at the center of geopolitical orders, periods of international stability that facilitate capital accumulation and the diffusion of the world system to new markets. Without hegemonic power, the world-system would be incapable of proliferating. However, this supposed integrality of hegemony and other particular components in the capitalist world-economy has led some to criticize WST as being deterministic and, ironically, state-centric.

### Critiques of WST: Determinist, Functionalist, and State Centric

As already mentioned, world-systems theory is far from unanimously accepted as the way the modern world works, and in fact, has been chastised for being both deterministic and obsessed with the global scale. Harvey's main argument against WST is that it comes too close to cornering geopolitics into a formalistic interpretation, a deterministic and stylized method that ignores much of what happens within the state – it fails to focus on class conflict (Harvey, 1987). The irony in his argument is that world-systems theory does in fact account for class conflict but as a separate institution from the state. Harvey continues his lamentation by stating that world-systems theory fails to address ways that capitalism embeds its internal contradictions in the geographical transformation of the landscapes of production, exchange, and consumption (Harvey, 1987). However, as already discussed, internal contradictions *are* accounted for in transformations brought about by political cycles and economic waves. The cycles and waves of competition epitomize change and dynamism in the world-economy and result in uneven development.

As previously alluded to, Marston (2000) has some insightful disagreements with WST as well, primarily with Taylor's adaptation of it to geography. Marston (2000, p. 228) notes that Taylor's "insightful attention to scale is largely descriptive" and "provides little detail as to how they are actually produced or how they shape and transform each other." This lack of detail is worrisome to Marston, as she notes that scales may in fact be produced by more than ceaseless capital accumulation and therefore could be more dynamic than represented in Taylor's framework. Most likely academics will forever argue that Taylor's dependence on capital accumulation to shape scale in the world-system is functionalist and misguided, but as Marston points out, Taylor's materialist framework "provides a well-spring for nearly all the work on scale in geography that has been produced since the early 1980s" (Marston, 2000, p. 228). Few could argue that Taylor's theory of scale has not been useful.

Other critiques of world-systems theory are far more problematic, particularly when those critiquing the theory are supposedly "sympathetic to its aims" (Skocpol, 1977, p. 1076). In one of the most formal and comprehensive critiques of world-systems theory, Skocpol (1977) argues that the theory is deterministic – Wallerstein's world-market plays too fundamental and all-inclusive a role in world-politics. She argues that WST "deprives politics of any independent efficacy, reducing it to the vulgar expression of market-class interests" (Skocpol, 1977, p. 1080). With more than a hint of irony, Skocpol (1977) notes that even though Wallerstein's goal is to create a theory that overcomes the shortcomings of modernization theories, he has instead produced a theory concentrated on dominant states and global political domination. Overall, she believes that WST's reliance on economic cycles, and the world-market in general, misses other fundamentally important variables in politics, namely: preexisting institutional patterns, threats of rebellion from below, and geopolitical pressures and constraints (Skocpol, 1977, p. 1080).

Though Skocpol's famous critique certainly addresses several shortcomings, WST has since evolved. The deterministic argument, though not unfounded, is misinformed. Though the world-system is inescapable, and though not everyone can partake in core processes, who gets to be exploitive, and how people will be exploited, is very much undetermined at any given point of time and constantly evolving. The constraints are not the world-system or the three scales but, rather, availability of raw materials and resources. As this thesis will demonstrate, WST certainly leaves room for independent political agency, but argues that it takes place within the world-economy, and therefore cannot escape market influences. Furthermore, her accusation that world-systems theory ignores fundamental variables in political agency is counterfactual. The fundamental variables not only exist, but they directly influence both the politics and the dynamism of the capitalist world-economy from within.

## Why World-Systems Theory?

Though numerous critiques of WST exist, it is the theoretical structure that will be utilized by this thesis for a variety of reasons, though primarily: 1) its holistic approach to political conflict from the local to the global; 2) its insights on the interactions of inter-dependent political institutions operating across all scales; and 3) its single world-economy model, which as will be shown, helps explain hegemonic extra-territoriality, consensus building, and the power behind the network metageography. Furthermore, as the rest of this chapter will attempt to illustrate, WST provokes and offers the potential to discover answers to particular questions important to this thesis, including: 1) how and why the role of the state is evolving in the world-economy; 2) why the U.S. is a prime target of anti-systemic movements and sub-politics; 3) what new political agencies represent and why they are gaining power; 4) how new politics are organizing themselves spatially; and 5) what impact the nodal network of virtual space has on political agencies operating across different scales. Because it offers both a horizontal scope for analysis of political processes and a vertical scope to cover all levels of scale, WST lends itself to critical geographic examination of conflict between the U.S. hegemony and other political agencies in the world – from the Communist Party to hackers.

Thus far we have been tracing a broad outline of world-systems theory and its utility in providing a geohistorical framework – through both scalar and temporal dynamics – for the analysis of social, economic, and political processes. This thesis is primarily concerned with the interactions between two agencies operating within the capitalist world-system: the United States as *world hegemon*, a territorial-based entity functioning at the scale of reality, and online *anti-systemic agents*, functioning through all scales and organizing in an open network. This chapter will now review definitions of world hegemony and explain the role and powers of hegemony in the capitalist world-economy through analysis of the hegemonic cycle. This will carry into analysis of the causations of, and processes behind, anti-systemic movements and a review of why such movements often end up targeting the hegemonic power.

## World Hegemony

"In Orwellian terms, all states are created equal but some are more equal than others" (Taylor, 1996, p. 22). This being the case, a state experiencing hegemony is the most equal state of all. Though various interpretations of hegemony abound in the social sciences, all stem from the word's Greek origin, *hegemonia*, and most share at least one of the origin's two definitions: 1) dominance of one political force over others, or 2) a guide, a political leader (Taylor, 1996, p. 24). Concerned mostly with the internal dynamics of the state, Gramsci's famous use of the term draws on the first definition (Gramsci, 1971), whereas WST generally incorporates the second – the holistic view of a single state garnering the power to be political leader of the world-system (Taylor, 1996; Taylor & Flint, 2000, p. 34-35).

However, interpretation of world hegemony is hardly binary. Gramsci's version of hegemony is often more prevalent than the state-centric one utilized by WST, and today many contemporary geopoliticans follow Cox's derivation of Gramsci's definition (Agnew, 1998; Agnew & Corbridge, 1995; Keohane, 1984). Cox views hegemony as a unique political domain stemming from global-scale shifts in social organization (Cox, 1981). Power relations within the world-economy maintain such a political domain, or order, through routinized ideological practices that become unfeigned by civil society at large (Agnew & Corbridge, 1995). Thus a geopolitical world order, or metageography, becomes obvious and true by all those involved – even those being exploited by core processes.

While thoroughly embracing the concept of an international political economy akin to Wallerstein's capitalist world-economy, Agnew and Corbridge (1995) subscribe to Cox's definition of hegemony. Essentially, they disagree with an all-powerful state approach to hegemony, arguing that hegemony does not necessitate a single organized territory but rather may be comprised of a cohort of elites in different states (Agnew & Corbridge, 1995, p. 17). In his own work, Agnew goes on to articulate even more clearly that hegemony may disproportionately benefit a single state, but that in reality "hegemony refers to the nature of the dominant social practices in a given historical epoch and how they bind together the various actors into a global society" (Agnew, 1998,

p. 55-56). The economic, cultural, and political “costs and benefits” of hegemony may concentrate in certain fortunate states, but in general they are distributed among all who “subscrib[e] to the contemporary principles of international life – irrespective of their geographic location” (Agnew, 1998, p. 56).

Like Agnew and Corbridge, Keohane utilizes Cox’s interpretation as well. However, unlike the others, Keohane takes a state-centric approach, viewing hegemony as “a single state strong enough to preserve and protect the essential rules that control the interstate system” (1984, p. 34). He argues that what underlies world hegemony is a powerful state’s willingness to take responsibility for the maintenance of the world-system. The center of Keohane’s argument lies with a hegemony’s “[decision] to exercise leadership,” which Keohane sees as “necessary to activate the posited relationship between power capabilities and outcomes” (1984, p. 34). He goes on to contend that a hegemony in crisis actually represents a crisis for capitalism, and that inter-state consensus has less to do with hegemonic extra-territoriality than “the common interests of the leading capitalist states” becoming “strong enough to make sustained cooperation possible” (Keohane, 1984, p. 43). He does acquiesce to Agnew’s perspective, however, arguing that hegemony is dependent on elites in peripherally dominated areas being aware of the fact that they are benefiting from the stability of the geopolitical order (Keohane, 1984, p. 45).

Even more state-centric in his approach, Modelski argues that by concentrating too heavily on factors of the world-economy, WST ignores “the little problems that leadership must cope with” (1987, p. 17). In his view, hegemonies are powerful states that gain world power in the political realm – not necessarily the economic sphere. Each world leader goes through political cycles of dominance lasting approximately 100 years (Modelski, 1987). The cycles that he proposes roughly correlate to paired Kondratieff waves, but no causal existence behind the cycles is noted. Herein lies the problem: in place of world economic factors, Modelski never successfully defines what the driving force is behind his political hegemony. Thus, though he observes some interesting trends in world-politics, his theory lacks causality.

In world-systems theory hegemony is more explicitly defined than in many structuralist arguments. Quite simply, the hegemony is a state that dominates economically in production, trade, and finance and uses this domination in procuring political power (Taylor & Flint, 2000, p. 35). Taylor and Arrighi argue that a key idiosyncrasy in WST's definition is that hegemony is viewed as an essential element proceeding through a particular cycle within the capitalist world-economy, and not as an independently powerful state in an anarchic system, e.g., with Modelski (Arrighi 1994; Taylor 1996, p. 26):

> "[T]he capitalist world-economy has evolved through rather long cycles we term hegemonic cycles. These are the eras that encompass the rise, achievement and subsequent decline of a hegemonic state and which define the changing nature of the whole system" (Taylor 1996, p. 25).

More specifically, "[h]egemonic states are particular core states that appear at specific conjunctures in the development of the world-system and are implicated in the overall development of the system" (Taylor 1996, p. 25). A key component in the world-economy, hegemony is instrumental in promoting the ceaseless accumulation of capital on which world-systems theory is based. The hegemony maintains economic advantage in production, trade, and finance through the exploitation of semi-peripheral and peripheral state markets (i.e., using cheap labor in the periphery to keep consumer prices low, or by *exporting technologically superior products* to peripheral markets, perpetuating a cycle of peripheral debt). As will be discussed, hegemonic states achieve this economic position of dominance through a cyclical process.

Hegemony is extremely rare. In the four hundred year history of the capitalist world-economy, there have only been three hegemonies: the United Dutch Provinces (UDP) in the 17th Century, the United Kingdom (UK) in the 19th Century, and the United States of America (USA) in the 20th Century (Arrighi, 1994; Taylor, 1993, 1996, 1999; Taylor & Flint, 2000). Though few in number, this is a sign of hegemony's strength, not weakness. Every hegemony comes to fore with an innovative new way of accumulating capital, dominates the world both economically and politically, and then declines. Even after the hegemony disappears, however, the systemic innovations live on. The Dutch mastered mercantilism; British hegemony was facilitated by the Industrial Revolution; and the U.S. has achieved economic greatness through mass consumerism (Taylor, 1993, 1996, 1999).

Without hegemonic powers there would be no capitalist world-economy, as every hegemon has played an intricate role in expanding capitalism (Arrighi, 1994; Silver & Slater, 1999; Taylor, 1993; Taylor, Beaverstock, & Smith, 2000). The world hegemony achieves the goal of expanding the capitalist system by continually promoting free trade with other states in order to accumulate more capital (Arrighi, 1994; Arrighi & Sliver, 1999; Taylor, 1993, 1996, 1999; Taylor & Flint, 2000, p. 67). Reaping gargantuan profits from their economic advantage, hegemonic states see only benefits in expanding the capitalist world-economy to new territories – even if historically, it always comes back to haunt them.

Geohistorical analysis of the three hegemonies demonstrates that the economic superiority behind their power is gained in a systematic order. First, the hegemon becomes a leader in production. This is often brought about through technological innovation, such as the woodworks of the Dutch, the industrial revolution in Great Britain, and mass production in the United States. Second, dominance in trade and commerce is established. The Dutch achieved this through establishing a mercantile fleet. The British continued this with their merchant marines. The United States mastered trade and commerce through innovations in managerialism and the invention of trans-national corporations (M. Taylor, 1999). Hegemonic ascension to economic superiority is completed with financial dominance. Financial superiority occurs because the state with the highest production capabilities and garnering the most commerce soon accumulates the most surplus capital (Arrighi, 1994; Arrighi & Sliver, 1999; Taylor, 1996; Taylor & Flint, 2000, p. 67).

Arrighi defines surplus capital as “capital that could not be invested profitably in the activities out of which it stemmed” (Arrighi 1994, p. 134). In other words, surplus capital is sheer profit in the truest sense – reinvestment of surplus capital will not reap any rewards, and therefore it must be used elsewhere. Often times it is used to finance loans to other states and institutions – helping to accumulate more capital for the hegemony over a longer duration. Arrighi notes it was Dutch hegemony that first demonstrated that "the systematic accumulation of pecuniary surpluses could be a *far more effective technique of political aggrandizement than the acquisition of territories* and subjects" (1994, p. 140-141, emphasis in original).

It was through dominance of trade and capital accumulation that the first hegemony was born – not vast territorial claims or profuse demographics. With states coming to the UDP for financial assistance, a large swath of territory with a large standing army was not necessarily needed (Arrighi & Sliver, 1999, p. 39-42). However, though surplus capital begets more capital, this will only occur if other states are open for free trade. It became *crucial* for hegemonic power that other states and political jurisdictions did not impede the flow of economic trade – as dominance in economic production, trade and finance is worthless if no one is willing to open their markets. Therefore, hegemony always attempts to sell liberalism to the inter-state system.

Yet world hegemony is more than purely economic domination of production, trade, and finance. World hegemons are social, cultural, and political leaders as well. They possess the most technologically advanced and efficient military capabilities. Hegemonic powers are champions of liberal causes, as liberal policies open up more markets for capital exploitation. A world hegemon is dominant enough to coerce or induce the consent of other states to follow it as the intellectual and moral leader of the world-system (Arrighi 1994, p. 28). Perhaps O'Tuathail defines it most concisely when he writes: "A hegemonic power like the United States is by definition a 'rule writer' for the world community" (1996, p. 61). How, exactly, a hegemony writes the rules, and why other states generally follow, has been the subject of much discussion.

The role hegemony plays in the evolution of the capitalist world-system changes pending its temporal position in the hegemonic cycle. In order to better understand how hegemonies come to lead and influence the world-economy, a summary of the cycle involved in a hegemony's envious rise and inevitable demise is needed.

## The Hegemonic Cycle

As the hegemony is a crucial component of the world-economy, the cycle that it proceeds through both influences and permeates all processes of the world-system. Following a brief description of where the hegemonic cycle fits into world-systems theory, as well as its role in influencing the evolution of the capitalist world-economy rather than merely being a product of it, this section will proceed to analyze the cycle's phases, dissecting them into two parts: systemic chaos and high hegemony.

Arrighi and Silver argue that, thus far, each hegemony has possessed idiosyncratic attributes that contribute to long-term systemic change. Though the capitalist world-system endows certain states with the ability to become hegemonic, Arrighi and Silver espouse that hegemony is anything but "the mere reflection of systemic properties" (1999, p. 26), and that in fact, hegemony always involves "a fundamental reorganization of the system and a change in its properties" (1999, p. 26). In addition to being fortunate enough to possess and maintain a disproportionately high amount of surplus capital, certain structural and institutional innovations have helped propel hegemonies to dominance. A hegemony successfully promotes globalization and free trade through consensus (Arrighi & Sliver, 1999). As states compete to become "modern" like the hegemony, they are coerced into financing their development, further cementing the dominance of the hegemony. Eventually, however, particular states begin to innovate on hegemonic technological and economic features; as through opening their markets, states are capable of importing, mimicking, and improving hegemonic advantages. Certain states develop into fierce competitors for the hegemony by becoming savvy in both economics and political leadership.

### Systemic Chaos

Hegemonies arise in the interstate system during periods of chaos (Arrighi, 1994; Taylor, 1996). Arrighi defines systemic chaos as "refer[ing] to a situation of total and apparently irremediable lack of organization" in the interstate system (Arrighi 1994,p. 30). Such chaos is usually due to international wars on a massive scale resulting from the previous hegemony's systematic decline. From the ashes of these wars new hegemonies are born.

Hegemonic decline is a lengthy process, occurring over the second B-phase of a Kondratieff cycle. The hegemony's decline begins when other core and semiperipheral states have *adapted both technologically and economically* for better maneuverability in the capitalist world-economy. In other words, hegemonic states begin to decline as other states begin to gain – economically and politically. Ironically, the ability for states to compete with the hegemony often stems from the liberalism and free trade policies exported throughout the hegemony's rise. As states continually attempt to emulate the world hegemon, they gain *access to the very technology* that helps the hegemon maintain its superiority. By innovating on the hegemonic technologies, state economies begin to develop into serious competition for the hegemonic state. Eventually, as surplus capital becomes increasingly difficult to obtain, the competition between states for the accumulation of capital becomes hostile. Thus, what was once viewed as distinctly advantageous for the hegemony – liberalism, free trade, and open markets – acts as a double-edged sword and comes back to undermine its own power-base.

It is this hostile competition that leads to systemic conflict often conducted via global wars. Yet interestingly enough, it never happens that states directly contesting the hegemonic power become the next hegemony (Taylor & Flint, 2000, p. 67-68). Instead, warfare provides the final kick to an already weakened hegemonic power, but at the same time eliminates numerous hegemonic challengers due to the enormous costs involved in participating in global conflict. History has shown that it is the declining hegemony's junior partner that is poised to take over the hegemonic reigns (Taylor 1993, p. 5).

As the hegemonic world-order begins to fall apart, the hegemony is commonly dragged into a costly land conflict, and seeks financing from a junior partner. Arrighi and Silver note that the hegemony goes from being a creditor nation – with the largest capital surpluses in the world – to a debtor nation over the course of the war; whereas its primary ally gains much surplus wealth (Arrighi, 1994; Arrighi & Sliver, 1999, p. 37-96). Taylor concurs, arguing that the new hegemon in waiting always fights a "good war"

(Taylor 1993, p. 5). It arms its allies, who in turn do most of the fighting. The hegemon-to-be limits fighting to naval actions – to help maintain open seas for trade – and the main theater in the global conflict is avoided until the final stages of the war so that it can control the conflict's resolution and reestablish the world-order under its leadership (Taylor 1993, p. 5). Due to the decimated state of the world around it, the junior partner quickly outdoes the hegemon in the three areas that made the declining hegemon hegemonic – production, trade, and finance. After the chaotic period, the junior partner emerges as world leader and, realizing its economic advantage, quickly embraces a liberal agenda in its assumption of hegemonic duties. Part of this agenda is willingly financing the rebuilding of states lying in rubble.

### High Hegemony

During periods of high hegemony, a hegemonic power rules through consensus with little or no need for coercion – threat of military force. Peter Taylor notes that "[h]igh hegemony is achieved politically when those wielding power within the hegemon use this opportunity to create a new world in their image" (1999, 2001, p. 31). Painting the world in one's own image is no easy task, requiring both consensus making ability and coercion. One way the hegemony procures such abilities is through the establishment of international *political institutions* (Arrighi, 1994; Hudson, 2000; Taylor, 1996). For example, though officially an international organization of states, the U.N. has been used as a fixture through which American influence can be channeled to provide stability to the world-system. Even the United States' main nemesis, the Soviet Union, was a member of this hegemonic tool. The hegemony always provides stability through institutional structuring, and the resulting global stability directly benefits the proliferation of free trade – in turn, hegemonic capital accumulation.

Peculiar things happen when a hegemony is at its apex and the inter-state system is stabilized; hegemonic leadership is accepted globally as a "fact of life" and a hegemon's innovations and ideas become accepted as "modern" – defining of an era (Taylor, 1996, p. 84, 119). During its apex, the hegemonic state maintains enough stability in the competitive inter-state system for “golden ages” to develop (Taylor, 1996, p. 83). For it is under high hegemony that global conflict subsides, and states begin emulating the hegemonic power in order to become more like it. Emulation requires the opening up of borders for trade with the hegemon, which in turn creates more surplus capital for the hegemony to finance. Whether they realize it or not, most states have little choice but to consent to the hegemony because, as Taylor notes: “During high hegemony other states are structurally in a position of economic dependence so that to resist the hegemon would have dire consequences for their economic well-being” (1996, p. 153).

Throughout history high hegemony has been limited in time and scope, with each successive hegemonic power maintaining hegemony for a shorter time but over an enlarged scale (Arrighi, 1994; Arrighi and Silver, 1999; Taylor, 1996). There are many reasons for the onset of hegemonic decline. Some attribute decline to pure economics – the hegemony becomes “overstretched” imperially and financially dependent on other states to maintain its military (Kennedy, 1988). Free trade spreads, but with it so do the ideas and technology that in the beginning provided the hegemonic power an advantage. Exportation of *technological developments* provides other states an opportunity to develop and innovate, indeed, modernize hegemonic technology, alleviating hegemonic dominance in particular economic arenas and fostering more inter-state competition (Taylor & Flint, p. 67).

Arrighi and Silver (1999) believe that the hegemonic cycle can be analyzed through the role of financing, arguing that finance is at the center of every hegemony’s rise and demise. Using geohistorical analysis to illustrate a pattern in every hegemonic cycle, they argue that there are three phases to hegemonic transition (Arrighi & Sliver, 1999, 37-96). First, the hegemony loses its monopoly over the open seas, often needing to make alliances with regional sea powers to enforce its world order (Arrighi & Sliver, 1999, p. 37-96). Sea power is a necessary component to ensuring open trade around the globe, and thus, by needing to depend on other powers’ for assistance, the hegemony’s ability to coerce begins to diminish. Second, the economic innovation lying behind hegemonic ascension – for the Dutch, mercantilism, the British, industrialization, and the

U.S., mass consumerism – actually begins to undermine hegemonic superiority, as other states master the techniques, innovate, and compete (Arrighi & Sliver, 1999, 37-96). Finally, with hegemonic advantages in production and trade diminishing, the time is ripe for competition over surplus capital to climax in global conflict. Financing is often the last stronghold for the world hegemony, but at the end of a costly war, it finds itself in debt to its allies and no longer hegemonic (Arrighi & Sliver, 1999, 37-96).

For the United States high hegemony began grinding to a halt in the 1960s. As it entered the Vietnam War, the U.S. demonstrated a dire inability to beat back popular resistance – neither at home through consensus or through coercion in Vietnam. During this time, the United States not only went into its first economic recession since assuming hegemony – and would never be capable of regaining its once monopolistic dominance over the world economy – but drastic and reactionary policy changes, such as giving up the gold standard in 1972, signaled the beginning of the end for U.S. high hegemony (Agnew, 1993). As Wallerstein notes, “The United States suddenly became aware that the coffers were not bottomless” (Wallerstein 1987, p. 20). Other surging semiperipheral and core states began to dominate traditional areas of United States production. As the Vietnam War proved more costly, surplus capital began pouring out of the United States to other countries, who in turn financed the U.S. war.

Yet, hegemony does not erode easily. Since the Vietnam debacle, U.S. hegemony has steadfastly maintained the reins of world-leadership. Serious economic challenges have come and gone, but all have been incapable of dismantling a particular social and cultural power that the U.S. holds over the world-economy. There are other forces at work for U.S. hegemony, forces that economic competition has not found a way to circumvent, yet.

## Modernity and Universality

To expand free trade and become the most efficient economy in the world-system, the hegemony must push its sovereignty beyond its own borders (Hudson, 2000). There are several ways of gaining this extra-territoriality; though, of particular interest to this thesis is the expansion of hegemonic sovereignty through the exportation of modernity. Modernities vary with time and place. Taylor defines modernity as the “taken for granted belief that we are modern,” which is “embedded in everyday thinking and behavior” (1999, p. 4).

Though a multitude of modernities proliferate in the world, the epitome of what it is *to be modern* is found in the everyday world of the hegemony (Taylor, 1999, 2001). This has been true throughout the history of the capitalist world-economy. Thus, modernities actually function as social tools promoting hegemonic expansion of cultural power (Taylor, 1999). Taylor argues: “A hegemonic agent is the producer of a particular modernity” (Taylor 1999, p. 29). The reason that modernities exist, and the concept of becoming modern is embraced by political institutions around the world, is due to the cultural dominance of a given world hegemony. Yet in addition to cultural superiority, *technology plays a key role*: “The hegemon is the ‘high-tech’ champion of its age and this advantage is projected beyond politics and economics to define the leading world ideas” (Taylor 1996, p. 85). Technological and social innovations and the application of these new inventions tend to agglomerate both temporally and spatially within the hegemonic cycle (Taylor 1996, p. 85, paraphrased). Each hegemony produces a technological feat that no other state of the same era is capable of replicating: the Dutch reclaimed incredible amounts of land from the North Sea; the British showed off their technical superiority in the Great Exhibition of 1851; and the United States put a man on the moon (Taylor 1996, p. 87).

The world hegemon exports what Taylor calls a *prime* modernity “because of [the modernity’s] direct association with the world hegemony” (Taylor 1999, p. 32). It is the prime modernity because the hegemony is able to diffuse it to the entire world (Flint, 2001, p. 769-770). Such hegemonic projection is facilitated through the process of emulation. By simply exporting to the world-market, the hegemony will offer other states cultural, social, and technological products to covet. In turn, states will consume this modernity in the hopes of becoming like the hegemon. This unwittingly allows hegemonic social and economic sovereignty to expand over other states’ territories.

During Dutch reign, mercantilism was the prime modernity being emulated; under the British, industrialization; and currently, Americanization, i.e., globalization and suburbanization, the process of exporting the culture of mass consumerism (Taylor, 1999, p. 56-59, 109-124; Taylor & Flint, 2000, p. 367).

More to the point, in addition to exporting an economic way of life, prime modernity sells a social system. During U.S. hegemony this has traditionally been one that is white, middle class, patriarchal, and suburban (Taylor, 1999). Such social systems are often exemplified through hegemonic art forms: Dutch paintings, British novels, and American cinema have all played a role, during their respective eras, in proliferating what it is to be modern (Taylor, 1996, 1999). For example, American films often illustrate the American Dream and display the victory of the common person – through images of the open road, suburbia, and the joys of consumerism (Taylor, 1999). The multi-billion dollar film industry not only accumulates capital by making entertainment a commodity, it continually exports and reinforces a social *image* to the world of what it is like to be – indeed to live – modern. This is not to say that it necessarily presents a positive image either: gender roles, racial stereotypes, environmental preferences, all such things are diffused through the prime modernity as illustrated in contemporary Hollywood (Taylor, 1999).

Prime modernity will evolve during the course of a hegemonic cycle. The recent television shows "Beavis and Butthead" and "South Park" both illustrate what it is to be modern as much as "Leave It to Beaver" – though far more ironically, critiquing the American Dream. Nation-states consume the exported prime modernity as social, political, and economic ideals to mimic; they consume out of a covetous desire to become akin to the hegemony. The hegemony, in turn, derives its power from other states' desire. It suggests that countries consensually open up for trade – if you import, modernity will come. And so, through economic dominance, liberalism, and prime modernity, the world hegemony is capable of stretching its sovereignty beyond its own borders into other states. This extra-territorial influence is a crucial component in establishing a stable world order conducive to the unimpeded accumulation of capital.

### Sovereignty Versus Extra-territoriality

Sovereignty is an integral component of the inter-state system. Originating under Dutch hegemony with the Treaty of Westphalia, the concept of sovereignty granted territorial states the infallible right to govern and control commerce within their own demarcated borders, or as the dictionary summarizes succinctly: "complete independence and self-government" (Davies 1970, p. 667). Sovereignty is "based on the acceptance of rights to absolute exclusive private property" (Hudson 2000, p. 279). As an accepted and recognized institution of the capitalist world-economy, sovereignty allows state agencies to compete with one another in the accumulation of capital. Hudson visualizes sovereign states as pieces of a "regulatory landscape":

> "Regulatory landscapes are spatial organizations of economic activity and political regulation, which are geographically structured through the use of borders and territoriality[.] Most importantly, regulatory landscapes are socially constructed or constituted, and scaled in particular ways" (Hudson 2000, p. 273).

Hudson goes on to hypothesize that scale is crucial to understanding sovereignty. Scale is influential in the creation of boundaries, and in turn, only accepted boundaries provide the power to be inclusive and exclusive (Hudson 2000, p. 273). Hudson notes "scales and borders rarely change because they are institutionalized through laws based on territory" (Hudson 2000, p. 273). Scales and borders in the world-system are based on the territorial state.

The hegemony plays a key role in creating the institutions that help reshape the regulatory landscape of the world-system. As with Dutch hegemony, which helped forge the concept of territorial sovereignty, the United States' hegemonic process has had a direct impact on sovereignty – diminishing sovereignty's role in the inter-state system through the exportation of its prime modernity – Americanization and mass consumption. Americanization lies behind contemporary globalization, utilized as a tool to diffuse U.S. power through the opening of new markets to the world-economy. Hudson argues that the "central feature of [the] processes of globalization [is] the reshaping of regulatory landscapes” (2000, p. 273), or as he put in simpler wording: “Globalization … is best understood in terms of changes in the importance and meaning of space, place, distance, and borders” (2000, p. 272).

There are two prime aspects to sovereignty: political regulation and economic activity. Disputes over political regulation often result in border conflicts; whereas, disputes over economic activity are played out in debates over wealth distribution and trade wars (Hudson 2000, p. 275). Being the most powerful state in the world-system, the hegemony establishes institutions that help exert its economic sovereignty into the territory of other political sovereigns. This hegemonic power is called extra-territoriality – the extension of one state’s sovereignty over others’ borders. For example, during high hegemony the United States established the International Monetary Fund, World Bank, and the United Nations as institutions that exert influence in other territorial sovereigns for the benefit of stabilizing the hegemonic order and facilitating the fluid movement of capital goods. Institutional creation – wherein other states participate – also gives the hegemony political advantage over the inter-state system, in that the institutions lend legitimacy to hegemonic extra-territoriality. Hudson notes: “Contests over sovereignty are about which/whose rules should rule in which space … in relation to which activities; they are battles over the appropriate scale and scope of political regulation” (2000, p. 275).

As already discussed, a fundamental component of the hegemonic cycle is the hegemony’s insatiable desire to spread free trade and expand the world-market in order to accumulate yet more capital and increase the global consumer base. However, under the institution of sovereignty, other states are theoretically capable of refusing to allow the flow of economic goods across their borders. In order to overcome this paradox between economic desirability and political reality, the hegemony champions the free movement of commodities across all sovereign borders while at the same time satisfactorily maintaining the concept of territorially based political institutions. The hegemony gains access to the economic resources of other states, through institutions such as the IMF and World Bank, but concurrently argues for its own and others’ political sovereignty. If not falling in line with the hegemony's world order, institutions may be used to strip particular states of their political sovereignty as well (e.g., Iraq and Serbia). Through the use of these newly invented institutions (e.g., U.N., NATO, et cetera), the hegemonic power and its allies are often able to expand their jurisdiction of political regulation into other states' territory, without acquiescing any of their own. Such expansions of influence represent the power of extra-territoriality.

The United States has been particularly successful at diminishing both economic and political sovereignty in the world-system for its own benefit. At the beginning of U.S. hegemony, borders were all important, as the world was organized into national economies (Hudson 2000, p. 274). In such a regulatory landscape, not only did rules and regulations not spread beyond borders, economic transactions were controlled as well. Now at the end of its hegemonic cycle, however, a dichotomous power struggle is taking place within the world-economy, as contemporary globalization is promoting a global political economy where borders become far less significant – political regulations and economic transactions are losing their territorial reference points or applications (Hudson 2000, p. 274). "The unbundling of territoriality is central to the current phase of georegulatory change, as it allows an increasingly borderless economy to coexist with a political system based on borders and sovereignty" (Hudson 2000, p. 275).

This unbundling of territoriality – hereon also referred to as "deterritorialization" – has dire implications for any forthcoming hegemonic cycle, as the contradictions between regulatory and economic sovereignty become more blurred and contentious. With United States hegemony in decline, reviewing deterritorialization's impact on the evolution of the world-system leads to a startling projection – a capitalist world-economy in crisis, a capitalist world-economy teetering on the verge of a new form of social structuring. As the United States has successfully subverted traditional forms of national economic sovereignty through the process of globalization and the exportation of its prime modernity, it has potentially undermined future hegemonic cycles within the world-system by burning the bridge that brought it to world domination (Agnew, 1993; Taylor, 1993). Hegemony requires territorial sovereignty to forge economic dominance, and in the waning phases of the U.S. hegemonic cycle, sovereignty's role in the world-economy has been dramatically reduced and redefined. One area of the modern world where this development is most obviously manifested is in both economic and political agency in cyberspace, or even more precisely, in the anti-systemic agencies utilizing the Internet against territorial regulation.

## Anti-Systemic Movements

There is a truism running through all society in the capitalist world-economy: "People resist exploitation. They resist as actively as they can, as passively as they must" (Amin et al., 1990, p. 27). Resistance to the American Dream in the 1960s and 1970s signaled the end of U.S. high hegemony. Protestations by numerous peoples peripheralized within and outside the United States hegemony thrust the inherent contradictions behind U.S. prime modernity and leadership into the limelight for the world to see.

In *Transforming the Revolution*, Wallerstein argues that anti-systemic movements are often sparked by contradictions surrounding the ideals of liberty, equality, and freedom, and this proves itself particularly true in the case of the baby-boomer movements (Amin et al., 1990). Even though success was limited and short-lived, Wallerstein sees 1968 as a major turning point for anti-systemic movements in that they launched a strategic debate about how best to transform the world-system. Traditional social movements – social democrats, communists, and the national liberation fronts – had proven themselves incapable of transforming the system, having taken control of state units and subsequently withered in purpose and achievements (Amin et al., 1990; Taylor, 1991). Thus, disorganized rebellious movements, primarily comprised of students, banded together and confronted the hegemony by agreeing on a "middle-run strategy" – they formed a plurality of social movements (Amin et al., 1990, p. 39-40).

The civil rights, anti-war, and feminist movements, collectively referred to as the "new social movements" by Wallerstein (1990), signalled an end to hegemonic leadership through consensus at the very roots of the hegemony's power base. The civil rights movement displayed contradictions in the American Dream; it internally contested the modernity that the United States was exporting to other states – concepts of equality and liberty. The anti-war movement showed a growing disenfranchisement with hegemonic rule; it attempted to offer an alternative modernity to mass consumerism. Unlike in past hegemonies, where social movements had little immediate or long-term influence, these contemporary anti-hegemonic movements quickly induced repercussions within the hegemony that last to this day.

Though the different sub-movements fought over various issues and for different peoples, for the first time in the history of social movements, most of the disparate parties communicated with and supported one another. Furthermore, unlike with past movements (e.g., communist and national liberation fronts), the new social movement rejected the notion of securing state power to implement changes. Much to territorial states' chagrin, movements began organizing their causes trans-nationally, largely ignoring inter-state borders. Learning from the debacles of history, the new social movement realized that spontaneous uprisings are not viable as a serious method for social revolution (Amin et al., 1990). Securing state power was not enough either, as even though it allowed power over processes within a territorial jurisdiction, it failed to change the system as a whole; the capitalist world-economy is capable of working around dissident states (Taylor, 1991). Wallerstein notes that transformation of society requires new social organization, and what sets the new social movement apart from historic ones is its attempts to achieve organization through various popular "universal" issues – e.g., environmentalism, feminism, and civil rights (Amin et al., 1990).

In their analysis, Silver and Slater also conclude that social discord plays an intricate and fundamental role in the process of hegemonic decline. With dire implications for U.S. hegemony, they note that social history appears to be speeding up – social changes are affecting states and hegemonies more rapidly than they did in the past (Silver and Slater 1999, p. 215). While the hegemony attempts to ensure stability in the world around it – through coercion if necessary – social conflict often ignites at home. Silver and Slater see a process similar to this in all three hegemonies' eventual demise – the breakdown of what they term the hegemonic social compact (1999, p. 214).

During its hegemonic ascension, the U.S. offered a "New Deal" to various anti-systemic movements in order to quell any threat they might eventually pose to high hegemony (Silver & Slater, 1999, p. 283). It was a social compact between the hegemony and the anti-systemic movements of the day, promising the working class "security of employment and high mass consumption" and offering elites in the periphery the right to self-determination and loans to catch up with Western modernity (Silver & Slater, 1999, p. 283). Of course, this social compact was, in the long run, untenable and could not be met indefinitely. The ensuing letdown of expectations eventually led to the development of new social movements against the prime modernity.

Silver and Slater view the beginning of the breakdown in the social compact, and the subsequent decline of the United States, as beginning with the civil rights and Third World movements of the 1960s (1999, p. 214). Attempts by the United States to quell and quiet these revolts only intensified the fiscal crisis stemming from the Vietnam War. While the U.S. was losing its economic dominance, social angst toward the fallacy of the American Dream heightened at home. The social movements of the 1960s, particularly those against the Vietnam War and for civil rights, demonstrated that the American Dream was not universal, not even in the U.S. The "climax" of hegemonic decline, according to Silver and Slater, can be found in the Iranian Revolution and subsequent hostage crisis of the late 1970s and early 1980s (1999, p. 214). The United States went into a deep recession and peripheral states began thumbing their noses at the international order.

Social contestation grows precipitously at the end of a hegemonic cycle due to the instability of a world-order suddenly lacking strong leadership. Certain institutions come to compete with the hegemon politically and socially. The hegemon loses its legitimacy and its ability to exert influence over other sovereignties. Its institutions are seen as fallible. However, perhaps even more tellingly, the hegemony loses its high culture status. Taylor and Flint ardently oppose the view of a hegemony as "simply the location of the most efficient econom[y] of [its] time" (Taylor & Flint, 2000, p. 343). Hegemony is dependent upon a delicate equilibrium of economic, cultural, social, and political leadership, with each realm of leadership capable of destabilizing the world-system if the hegemony loses its ability to forge control through consensus.

Historically every run of the hegemonic cycle undermines certain institutions that give the capitalist world-economy its vitality. Frank believes this is where social movements play a fundamental role in transforming the world-system and perhaps the future of hegemony (Amin et al., 1990). Frank argues that as institutions within the world-economy and inter-state system become increasingly incapable of dealing with the rapid economic and social transformations occurring during the course of the Kondratieff wave and hegemonic cycle, social movements “replace or supersede some other institutional forms of social expression and action” and “intervene to transform existing, or form new, social institutions themselves” (Amin et al., 1990). This idea will be covered further in the next chapter, through analysis of theories on reflexive modernization (Beck, 1992; O'Tuathail, 1998).

Arrighi adds that it is through the expansion of the liberal agenda that each hegemony eventually contradicts and makes illegitimate the institutions maintaining its position of power – inducing the growth and wrath of anti-systemic movements (1994, p. 325). State sovereignty has eroded under U.S. hegemony due to its success in exporting neo-liberalism, and thus, the capitalist world-economy has evolved into a system *not dependent* on trade between national economies but transnational corporations (Agnew, 1993, p. 229-235; Taylor, 1993). As U.S. hegemony is established on the institution of sovereignty, it has inadvertently severed its own umbilical cord to continued hegemony. As each swing of the hegemonic pendulum fails to return the structure of world politics to where it was, more complexly formed structures and institutions of governance will come to fruition (Arrighi, 1994, p. 330).

The process of Americanization has ushered in numerous innovations and adaptations to the political structure of the world-economy, some of which may lead to the formation of an “ultra-hegemony,” a hegemony above the scale of the nation-state (Taylor, 1996, p. 186-187). Such innovations develop under U.S. tutelage as attempts to reestablish control over anti-systemic forces. However, Silver and Slater argue that even though financial expansion and reorganization of the world-economy effectively disrupted the movements of the 1960s, contradictions with the hegemonic compact remain unresolved (Silver & Slater, 1999, p. 284). As the U.S. continues its hegemonic slide, new social forces that will be even more difficult for the U.S. to subjugate will be unleashed (Silver & Slater, 1999, 284-285). Even as economic restructuring sugarcoats labor conflict in the core states, new agencies will eventually blossom over the same and, as will be shown in the next chapter, new areas of unresolved conflict (Silver & Slater, 1999, p. 285).

Interactions between online social movements, particularly those aimed against U.S. hegemony and its prime modernity, symbolize a new level of interconnection between various social networks that were previously territorially affiliated. As will be discussed in the next chapter, due to lack of territoriality, online anti-systemic movements may play a pivotal role in transforming political agency in the capitalist world-economy and subjugating continued U.S. hegemony.

## Conclusion

The relatively new and rapidly expanding virtual world, with its nodal structure and networking capabilities via nearly all platforms of communications devices, has had a tremendous and immediate impact on speeding up the process of globalization – through commerce on the Internet. Cyberspace provides a new geography where economic transactions, particularly knowledge and information commodities, can take place without the intrusion of regulatory borders. It is also ushering in the potential demise of political sovereignty – by allowing deterritorialized political agencies to cross state borders with impunity.

It is the U.S. hegemony's ceaseless attempts to change the economic aspects of sovereignty so that borders are no longer impediments to fluid capital accumulation that is "[introducing] tensions between the scales of economic accumulation and political regulation" (Hudson 2000, p. 275) and opening the U.S. to anti-systemic backlash. The capitalist world-economy needs the state system in order to continue existing, as its means of expanding the ceaseless accumulation of capital is through the hegemonic cycle – a cycle based on the political institution of the state. Yet at the same time, both online economic growth and political activism in the waning days of American hegemony stands in direct contradiction to the territorial sovereignty of the state system. As will be discussed in the next chapter, there are “no boundaries” in cyberspace (Castells, 2000; Everard, 2000; Himanen, Castells, & Torvalds, 2001). In the virtual realm, traditional political regulation based on territory is inconsequential. The network structure of the Internet is threatening to act as a subterfuge to established hegemonic institutions, based on territoriality, that help the U.S. gain from its prime modernity.

The politics of globalization have now spread into virtual space, a global network from which new political agencies can join in the fray of international political conflict. This new unregulated arena of political contestations offers social movements the option of political agency equal to that of the U.S. hegemony and at a scale beyond hegemonic control (Himanen et al., 2001; Wray, 1998). In other words, the potential for navigation and infiltration at various points in the nodal network is equal between hegemony, a trans-national corporation, a non-government organization, and a privileged Palestinian sitting at a computer in the West Bank. Political ability in virtual space is not dependent upon size of army and strength of borders; any person connected to the global network can take part in systemic political activities (Everard, 2000).

As economic superpower, the hegemony’s interest lies not in expanding its political regulations over other states through the acquisition of territory, but rather from “promoting and protecting a liberal world economy” through prime modernity and extra-territoriality (Taylor 1993, p. 7). However, this presents a major paradox for continued U.S. hegemony. The hegemonic cycle has expanded the capitalist world-economy to a realm beyond its institutional regulatory abilities, and meanwhile, it has potentially surrendered the role of national economies to trans-national corporations (Agnew, 1993; O'Tuathail, 1996, p. 228-229; Taylor, 1993, 1996). The technological innovation of cyberspace stemming from U.S. hegemony allows real world capitalism to expand into a virtual world free from state regulation impinging upon economic fluidity. Furthermore, it provides opportunity for anti-systemic political agencies to organize around and subvert political sovereignty upon which U.S. hegemony rests.

Even though states will begin to adapt to these new threats on their institutional power (Everard, 2000), or as will be discussed in the following chapter, will begin to “reflexively modernize” (Beck, 1992), the social and political repercussions of this period of evolution hold dire implications for the United States. According to Silver and Slater (1999), Arrighi (1994; Arrighi & Silver, 1999), Agnew (1993), and Taylor (1993, 1996), the United States is nearing the end of its hegemonic cycle. Contrary to appearance – the booming economy of the 1990s, a technologically dominant military, and its continued prime modernity – the United States has begun its descent into hegemonic decline. Though not transparent through economics alone, a look at the geopolitical landscape shows that global competition for power is once again approaching its apex.

Modelski (1987) argues that international stability proceeds through a cycle along with hegemonic power. During the global war, from which hegemony stems, there is a strong desire for geopolitical order, but no state is dominant enough to create one in its own image (Modelski, 1987). After the war, as has been discussed, a hegemonic power rises, and it quickly establishes a stable geopolitical order through a method of consensus making, which is dependent upon other states craving international stability after the destructive war (Modelski, 1987; Taylor, 1996). Under this new order, of course, the hegemony flourishes, but no long thereafter, approximately twenty-five years, other states begin to adapt and once again become more competitive (Modelski, 1987). Jealous of the hegemony’s privileged position, they begin to grumble and disregard certain aspects of the hegemonic order. Eventually, states and political institutions begin to backlash against the hegemony completely, often violently, and the world begins to slip into instability (Modelski, 1987). Today the United States is no longer capable of maintaining power through consensus, nor in many circumstances, even through the threat of force. Terrorist attacks on the hegemony represent one form of backlash – a new form, actually, as they are non-state based – but other, more traditional examples, proliferate: ally Israel disregarding U.S. demands; China and Russia signing a military non-aggression pact in Asia directed at the U.S.; the European Union going against hegemonic desire and supporting the Palestinians over Israel; et cetera.

On top of U.S. decline, many concur that the capitalist world-economy is heading toward a period of power transition (Agnew, 1993; Arrighi, 1994; Arrighi and Silver, 1999; Taylor, 1993, 1996) and a new type of political geography (Agnew, 1994, 1998, 1999; Taylor, 2000, 2001). Political networking around non-territorially aligned issues and the rise of the non-territorially affiliated trans-national corporation, represent contradictions that confront the continued existence of the world-economy, much less U.S. hegemony. The growth of the Internet, acting as both an economic innovation and a tool for political action, will play a crucial role in whether the U.S. prime modernity overcomes its own internal contradictions or in helping to usher in a new economic world-system. Much of this may be determined by political agencies using the geography of the Internet in their confrontation with a hegemonic power dependent on the traditional geography of classic geopolitics – a battle between two geographies, the nodal network versus territoriality.

## Chapter Three: Network Society and Online Agencies

As was illustrated in the preceding chapter, U.S. hegemony, and the cyclic process it proceeds through, is a fundamental and influential component in the capitalist world-economy. Through its establishment of political institutions, its creation and diffusion of technology, and its perpetual desire to expand the world-economy for perceived personal gain, the United States continues to shape the world-system, even as this very expansion whittles its hegemonic power base.

However, the end of the U.S. hegemonic cycle has seen the dawn of some dramatic changes in the world-economy, including for the role of the state within the system. Tele-communications technologies, most notably the Internet, have had a major impact on the potential influence and scope of political contestation amongst non-state actors. As states struggle to adapt to the political and social risks of the virtual world brought about during the latest Kondratieff wave, core and peripheral agents alike have been aggressively innovative in using communications networks to thwart the traditional authority structure of the inter-state system. As U.S. hegemonic decline brings with it instability to the world-system, a string of societal risks emanate from the shadowy fringes of cyberspace.

This chapter will discuss the emerging global network society, a new form of societal organization ushered in by contemporary communications technology that will have major implications on the evolution of political institutions in the world-economy. Within this discussion, Beck’s theory on reflexive modernization in risk society will be examined. This will lead into analysis of the Net (hereon also referred to as the Internet, cyberspace, and virtual world) by reviewing its history and role within the world-economy. In turn, contemporary forms and methods of anti-systemic movements and sub-politics utilizing the Internet to challenge state and hegemonic authority will be analyzed. The chapter will draw to a close by reviewing the challenges facing traditional state policy in the face of a rapidly networking global society. Throughout, special focus will be paid to the reflexivity of U.S. hegemony, as it both gains in extra-territorial power from the diffusion of the Internet around the world, but in the meanwhile, watches its own advantageous position place it in the crosshairs of anti-systemic movements.

### Metageographic Shift

Due to changes in sovereignty under the U.S. hegemonic cycle, as well as changes in economic transactions now that borders play less of a role in the world economy, some geographers have begun to argue that globalization is bringing about a change in metageography, a "metageographical moment" – a shift to a new way of viewing the world, a world seen as a space of flows and networks (Taylor, 2001, p. 3). Taylor notes that contemporary globalization appears to involve an evolution in the role of scale in the world economy and a "fundamental change in the nature of social space" (Taylor, 2001, p. 1).

Metageography is a term "to describe the geographical structures through which people order their knowledge of the world" (Taylor, 2001, p. 3). It is society's "taken-for granted world" (Taylor, 2001, p. 3). The metageography of the capitalist world-economy over the past four hundred years has been relatively consistent – that of a system based on territorial spatial units, states (Taylor, 2001, p. 3). Metageographical moments arise "when the old is eroded leaving a geographical opportunity for a new picture of the world to emerge" (Taylor, 2001, p. 4). Taylor believes that metageographic evolution is intricately linked to capital accumulation, or that is, the geographic infrastructure through which capitalism operates induces changes in how society structures itself (Taylor, 2001, p. 4). Therefore, perpetual accumulation of capital eventually begins to undermine the geographic structure (currently the sovereign state system) in which it has evolved. The most recent technological feat of the U.S. hegemonic cycle, the invention of networked virtual space, is a tool facilitating capital accumulation and leading to "the deconstruction of national financial and cultural boundaries which are an intrinsic attribute of [the modern world-system]" (Loader, 1997, p. 9).

Though all hegemonic cycles bring with them cultural and social changes (Sherman, 1999), the prime modernity of Americanization, or globalization, has begun not only to undermine United States hegemony but, potentially, the entire inter-state system itself (Taylor, 1993, 2000). The world's metageography is shifting from territorially based states, with the role of protecting national economies, to urban centers of economic power that are connected through networked technologies of telecommunications and transportation – regardless of state allegiance or boundaries (Mitchell, 1999; Sassen, 1991, 1994; Taylor, 2001; Taylor, Beaverstock, & Smith, 2000). At the center of this change lies the nodal geography of the virtual world, and the social and political opportunities that this new geography brings.

As this chapter will illustrate, concurrent with the societal shift in metageography, political agency changes as well. Beck argues that this current reshaping of politics in the world-economy is due to various "reflexive modernizations" taking place in state political institutions (Beck, 1992; O'Tuathail, 1998). As the foundations of industrial capitalism have become increasingly questioned, "the modern industrial institutions that have helped create our ongoing ecological, informational and security crises … are having to confront what they have unleashed" (O'Tuathail, 1998, p. 27). This has particular significance for the United States today, as it lies at the center of many cyber-attacks.

Reflexive modernization is the process of state-based industrial institutions "adjusting their missions and re-legitimizing their mandates" in order to maintain control over the geopolitical system during its evolution from an industrial society to a risk society (Beck, 1992; O'Tuathail, 1998, p. 27). During reflexive modernization, sub-politics often sprout. As institutions such as the state adapt to contemporary risks, they often relinquish some of their monopolies over particular forms of political power and knowledge production. Thus politics, knowledge, and new mediums begin to diffuse to different institutions and movements (Beck, 1992, p. 154). These new institutions and movements are sub-politics, agencies that are no longer under the yoke of old institutions of power and present a forum of opposition to contemporary risks.

The redistribution of political power during reflexive modernization is partially dependent on the ability to communicate to the masses and incidentally forge support around, what become, the most glaringly important problems or “risks” (Beck, 1992). Sub-politics originate around the most contentious contradictions of the world-system – environmental issues, polarization of wealth, globalization, et cetera (Beck, 1992). The advent of the Internet has presented one of the most potent mediums through which sub-politics can form, organize, and even take action, due to its nodal geography and lack of systemic control. In the past, due to state controls over communications, sub-politics were largely confined to the state or regional congregation, though anomalies such as global environmental movements did exist. However, with the network organizational structure of the Internet, sub-politics have increasingly become trans-national and highly integrated (Arquilla & Ronfeldt, 1999b, 2001b, 2001c).

As state and industrial institutions are increasingly challenged, socially, politically, and scientifically, they must either change, that is invent new institutions capable of handling the contested risks, or eventually face delegitimization. When established political institutions (e.g., nation-states) fail to adapt to handling contemporary risks, sub-politics mold around new institutions and venues – a prime example of which are the global anti-free trade groups (Beck, 1992; O'Tuathail, 1998). Sub-politics are an integral component of post-industrial risk society, and O’Tuathail argues that their rise under globalization signals a change in contemporary geopolitics, as institutions used to order the modern world “become overwhelmed by the immanent pluralism of risks” (O'Tuathail, 1998, p. 29).

As Beck and O’Tuathail help explain, the structure of political agency is changing, diffusing downward to sub-state agents (online social movements) and individuals, as well as upward to trans-national entities (corporations and supra-nations). However, both Beck and O’Tuathail fail to offer an in depth geographic interpretation of these contemporary changes. By using Beck’s insights on risk society within a world-systems framework, one can see that the current metageographic change to a network society is a product of reflexive modernization. This is evident in two places: 1) in the unimpeded rise of world-cities as the predominant centers of capital accumulation and finance, and 2) in the surge of online sub-political agents confronting state institutions through the medium of nodal, electronic space.

Though some in the social sciences have begun to question the future of the nation-state, it is premature to predict this dynamic political institution's demise. Instead, the state, and in particular the world hegemony, is in the process of adapting, or reflexively modernizing, itself to the coming geographic structure of the world-system. At this point, institutional changes in the way states operate are not necessarily good or bad, signaling the demise or rise of the nation-state, but exploratory and evolutionary (Everard, 2000; Himanen, Castells, & Torvalds, 2001). The current metageographic moment is all encompassing and the culmination of many factors, not simply a change in how technology is utilized for economic advantage. Everard notes that the use of new technologies does not necessitate a metageographic change, but rather, change comes from technologies' development into new processes through which humans live (2000, p. 75).

Castells (2000) concurs, arguing that information technologies are much more than tools to be applied for particular exploitive purposes, and act as processes in development of society at large. Castells' argument is that the current technological paradigmatic shift – ushered in during the U.S. hegemonic cycle and the B-phase of the Kondratieff wave – is inducing a societal move toward a network society (Castells, 2000; Himanen et al., 2001). The dawn of the network society is not occurring simply because of technology, however, but through the processes that new technologies produce in society at large – including the economic evolution from industrialism to informationalism and the societal reactions to it (Himanen et al., 2001, p. 157-58). Telecommunications technologies, in particular, are integral pieces within the social restructuring being brought about by the politics of contemporary globalization. As history demonstrates, the final stages of hegemonic cycles often produce technology capable of inducing societal changes in communication, organization, and identity affiliation (Everard, 2000, p. 76). Contemporary technological development is not a necessary component for networked organizational structures, but it most certainly has facilitated change toward new networks within society at large (Arquilla & Ronfeldt, 1999b, 1999c, 2001a, 2001b, 2001c). Like the telephone at the dawn of the twentieth century, which had a revolutionary impact on altering the social rules of organization and social structure within England, and eventually the entire world (Hugill, 1999; Martin, 1998, p. 69-70), many argue that contemporary telecommunications technologies are at the very least promoting, if not ushering in, a networked society (Castells, 2000; Himanen et al., 2001; Lenk, 1997; Mitchell, 1999; Sassen, 1998; Wellman, 2001).

Castells' vision of contemporary society's reorganization as a space of flows is an interesting one, but not without contention. Taylor laments that, though correctly interpreting society's rearrangement, Castells errs in his belief that this shift is solely a modern day phenomena (2001, p. 15). Taylor cites evidence that Castells' argument suffers from linear historicism, and that geo-historical analysis displays that "financial flows transcending states have been a cyclical phenomenon" (2001, p. 15). Agnew (1999), on the other hand, argues that though the geopolitical imagination of global society is steadily evolving to one that is nodal in structure, power has always operated in such a fashion. He contends that International Relations (IR) theories on political power have preserved serious flaws in social theory that do not correlate to everyday cognition (Agnew, 1999). These errors, Agnew (1999) argues, induce political theorists to treat power as a territorialized element, when in reality it is extremely mobile and always has been. Integral to the theme of mobility, cyberspace provides a borderless realm through which corporate interests and service industries are able to bypass the control functions of state borders.

During the B-phase of a Kondratieff wave, new technologies promote global economic realignment through the shifting of certain production from the core to periphery. Today, the production of knowledge and the accumulation of information have begun to replace the traditional roles of manufactured goods and raw materials, respectively, and also, labor and capital as the key resources in Western economies (Kitchin, 1998, p. 388). Brunn argues that the modern-state depends on information collection and knowledge construction more than ever to remain a viable political institution (Brunn, 1999, p. 109). Nation-states came to dominate as centers of power in production, trade, and finance through the self-recognized and upheld concept of sovereignty (Mann, 1997). However, globalization and technological processes have induced changes in the distribution of wealth and power in the world-economy based on an ability to innovate technology and circumvent sovereign controls on access to capital (Everard, 2000, p. 75). Herein lies an inherent contradiction. As states come to depend more on the production and unimpeded flow of information, the principle of sovereignty on which states are based continues to erode.

It must be made clear that a metageographic moment does not imply a complete dethroning of the old social structure for an entirely new and untested one. Over time, however, globalization continues to alter many of the traditional roles of the state, while allowing trans-national corporations avenues of escape from political regulation, and providing networked individuals the ability to become miniature political agents in the world-economy themselves (Everard, 2000, p. 52-53; Hudson, 2000). As society becomes more networked, the nature of power changes – becoming territorially unbound (Everard, 2000, p. 111-112). Cyberspace is one battlefield in the contested landscape of a new world metageography, and because of its inclusion of both state and non-state agents, the boundary between military and civilian political institutions is becoming blurred – particularly in regards to the categorization of online movements (Arquilla & Ronfeldt, 1999a, 1999c, 2001b, 2001c; Everard, 2000, p. 109-113). In addition to adding a whole new dimension to the world-economy, virtual space is creating a new world politics that dramatically influences the changing role of the nation-state.

Lying at the heart of state adaptations to network society are conflicts between anti-systemic and sub-politics using telecommunications technologies to facilitate their causes and states using it for continued exploitation and purposes of capital accumulation (Arquilla & Ronfeldt, 1999b, p. 74). Furthermore, while benefiting from informationalisation, the U.S. has been increasingly frustrated in its attempts to reflexively modernize its role in the network society so that it might cope with certain risks developing from these political processes that communications technologies invoke

(O'Tuathail, 1998, p. 26). The networked connections that rose to subsume the world during U.S. hegemony almost entirely ignore demarcated sovereignties, and thus, political agencies other than states are offered an opportunity to become mobile in a fashion that traditional, territorially bound geopolitical regulations and policies are incapable of stemming (Arquilla & Ronfeldt, 1999b, p. 74). In order to understand cyberspace's role in the world-economy, and the new form of politics it is helping usher in, we must first review geographies of contemporary communications networks – i.e., the geographies of cyberspace.

## The Internet, Cyberspace, and Virtual Reality: A Background

Though conventional wisdom and corporate marketing might lead one to believe otherwise, the Internet is actually a composition of numerous networks with hundreds of methods and formats for communication, of which the World Wide Web (WWW) is only one. Each system of networks has its own layers and levels of flows (Adams and Warf 1997; Brunn 1999). There is no traditional friction of space in the electronic realm, only information flowing between nodes in a nearly infinite matrix of connections (Graham, 1998; Kitchin, 1998). Various formats aside from the WWW are used extensively for both corporate and subversive reasons.

Perhaps the prime example of a system of networks within the Internet is provided by company *intranets*. An intranet is a private network connected to the Internet that only allows those within the private network access to the Net, not vice versa. Stephen Graham writes that intranets are becoming the fortresses of the virtual world (Graham, 1998). Sassen concurs, believing that corporations, with their potential to gather and secure vast amounts of information and knowledge, will use intranets as "citadels" of power within the Internet (1998a, p. 188). She goes on to argue that, the Internet by its very nature diffuses power sharing throughout its nodal space, making it extremely difficult to forge political monopoly of control over the entirety of flows within it (Sassen, 1998). Thus, the collision between civil society, which in general views the Internet as a libertarian space open to all, and corporations, who have a vested interest in securing some form of property control over diffusion of marketable knowledge and information, becomes a difficult one.

The exclusiveness of intranets does not go uncontested. In contrast to intranets hoarding information, knowledge, and corporate or government secrets, there are subversive systems in cyberspace helping certain agents undermine these systems' ability to do so. Numerous examples of alternative versions of the WWW exist, one of the most obvious examples being the now defunct Gopher system. Another more notorious Internet system is Hotline, which is used by online agents around the world to trade stolen information and knowledge capital (Tetzlaff, 1998).

As numerous academic definitions of cyberspace exist, it is unlikely that an exact lexicon will ever be settled upon. However, geographers, as scientists concerned with all things spatial, have attempted to rein in the Internet's lack of semantics. In general, cyberspace has been vaguely described as a landscape of digitized information (Luke, 1998, p. 286). Brunn describes it as being an infinite and nodal space, a chaotic network extending forever (Brunn, 1999, p. 113-114). Warf and Grimes further expand on this, viewing this infinite network as "neither inherently emancipatory or oppressive, it is a space of contested philosophies and politics" (Warf & Grimes, 1997, p. 1).

The lack of cohesion and utter chaos that characterize vying definitions of the Internet began when the system was still in an embryonic state of development. Established as nothing more than a state-funded communications network meant to survive a Soviet nuclear strike, the Internet evolved haphazardly, arbitrarily extending itself to various universities – predominantly on the West Coast (Adams & Warf, 1997; Castells, 2000; Kitchin, 1998; Lindsay, 1997; Warf & Grimes, 1997; Wray, 1998a; Wriston, 1997). Through the 1980s, the Internet was largely the realm of academic and technological elites.

Arguably, it was not until William Gibson's novel, *Neuromancer* (1984), that the first escapade of "cyberspace" extended into public consciousness. This award winning book, as well as other various pieces of successful science fiction, under the "cyberpunk" genre, began to mold the population's collective imagining of what cyberspace could be

(Clark, 1995; Fitting, 1991; Kellner, 1995; Poster, 1995; Stallabrass, 1995). Kellner argues that “Gibson [mapped] our present from the vantage point of his imagined future” (Kellner, 1995, p. 299). Science fiction writers began entertaining the idea of an anarchic network system – an uncharted, infinite nodal frontier (Burrows, 1997; Featherstone & Burrows, 1995; Stallabrass, 1995). Moreover, with the Internet becoming established in universities across the United States, academics began connecting to the system and using it as a tool in the dissemination of information and dialogues. The liberal underpinnings of the academic intelligentsia, coupled with the popular science fiction writings of an anarchic virtual future, led to the inherent perception of the Internet as an open channel for information and knowledge dissemination, even though in actuality it remained a state-supported, though unregulated, network for communication during nuclear holocaust (Balsamo, 1995; Lindsay, 1997; Sterling, 1993; Stone, 1995; Wriston, 1997).

The United States government eventually decided to stop funding the network and began privatizing the Internet in 1994. For the first time, corporations were allowed to sell portals into this virtual frontier. Coupled with the development of html code and the ensuing mass marketing of the WWW, techno-libertarians were suddenly forced to share their space with businesses interested in profit margins – a potentially volatile mix (Borsook, 2000). By the dawn of the 21st Century, the Internet was being transformed from a relatively free and open information network into a vast new consumer market with incredible potential for capitalist exploitation and great potential use for the declining hegemony. As the world-economy opened its way onto the Internet, regulation lagged far behind; like the Wild West of yesteryear, politics in cyberspace was largely dependent upon self-policing (Loader, 1997, p. 4). The U.S. government, much less local law enforcement agencies, was in no position to protect the public from crime in cyberspace, particularly when the criminals operated from overseas.

Luke (1998, p. 279) summarizes the discord in the geographic discipline over analysis of the Internet, noting: “Cyberspace problematizes a geography of space and place,” and therefore, numerous definitions and views of space continue to vie for ultimate acceptance. Much of this semantic competition centers around whether or not the virtual world is better defined as a place of interaction, a neutral space of flows, or both. Either way, the political implications of the Internet's role in the world-economy, and hence for the role of the modern-state, are gargantuan. The Internet is neither good nor bad, but it is most certainly not neutral (Everard, 2000, p. 53-54). It is a technological tool developed during the course of the U.S. hegemonic cycle and used for exploitation and neo-colonialist purposes by elites throughout the world-economy (Everard, 2000, p. 53-54; Nakamura, 2000). The Net has expanded U.S. extra-territoriality into households across the world (Holloway & Valentine, 2001). While contributing to globalization, Everard argues that cyberspace moves political power beyond the institution of the state (2000, p. 53), making it more fluid between the scales of local and global than ever before in history (Arquilla & Ronfeldt, 2001b, 2001c).

As can be seen, both definition and control of the Internet is contested, primarily stemming from the competition of use for the emerging nodal network – knowledge and information diffusion versus hegemonic extra-territoriality and state regulation (Lessig, 2001; Valeri, 2000). In order to understand online politics and conflict, it is necessary to correlate and contrast their spatial mobility to real world contemporary politics. In order to do this, however, it is imperative to first review Graham's three broad conceptions of interaction between the physical and virtual worlds.

## Social Conceptions of Cyberspace

Graham (1998) argues that three perspectives concerning aspects of space and place in communications technology dominate the social sciences. The first he calls the perspective of *substitution and transcendence* (Graham, 1998, p. 167). The dominant worldview right now, this outlook is highly deterministic and deemed by many to be utopian. It sees technologies as harnessing the potential to replace real world geography. It postulates that capitalist societies are becoming liberated from constraints of time and space, and that opportunities will exist to produce, or relocate, a place anywhere with the help of forthcoming virtual technologies (Graham, 1998, p. 168). The adherents to this school of thought argue urban areas will begin to decentralize as communications technologies eliminate the need for congregation of information and knowledge (Berry, 1976). This is a perception often marketed by technology corporations (Nakamura, 2000), and arguably it is a byproduct of prime modernity, or Americanization, as it sells the American Dream of being able to retreat to the country away from urban centers – a.k.a., suburbanization.

*Co-evolution* offers a second perspective on the spatiality of communications technologies, and is much more sophisticated in its exploration of how "the social production of electronic networks and 'spaces' co-evolves with the production of material spaces and places, *within* the same broad societal trends and social processes" (Graham, 1998, p. 171). Rather than strictly replacing real life with virtual technologies, Graham sees this perspective as more holistic, and less absolute in its predictions of change. New technologies offer humans more opportunity to de-localize themselves from the consciousness of reality around them, but they will still exist in that reality (Graham, 1998, p. 172). Society evolves with technology adapting to its uses, and abuses, but a definitive human-technology divide still exists.

This divide stands in stark contrast to the third popularly theorized perspective – the *cyborg*. Based on actor-network theory (Latour, 1993, 1998, 1999), the cyborgian perspective emphasizes human interaction with technology, but *not independently* from technology's reverse coaction with humans (Graham, 1998, p. 178; Haraway, 1991; Haraway, Penley, & Ross, 1991). Everything is an agent and reciprocal to other agents. Boundaries between humans and machines blend together. Social organization does not coincide with group modeling but is defined within various social networks (Wellman, 2001, p. 2031). Following the work of Haraway (1991), this philosophy views cyberspace as "a fragmented, divided and contested multiplicity of heterogeneous infrastructures and actor-networks" (Graham, 1998, p. 178).

The second perspective of co-evolution is the one embraced by this thesis. Not only does this approach allow for interaction between the institutions of the world-system in both the virtual and real worlds, but it also provides the possibility to view and analyze these interactions as processes in the holistic framework of the world-economy. The first perspective, one of techno-utopianism, is actually part of the hegemonic process of exporting consumerism and the prime modernity of Americanization – if everyone embraces technology, a libertarian world of equality predicated on having little need for the state as a political institution is envisioned (Bodow, 2001). This techno-libertarian perspective errs in viewing the virtual world as somehow unrelated and entirely alternative to the real world (Loader, 1997, p. 6-7). The cyborgian vision espoused by Haraway and promoters of actor-network theory, though being of use in some postmodern geopolitics (O'Tuathail & Dalby, 1998, p. 31-33), is difficult to use as a holistic analytical tool outside of defined case study scenarios. To analyze the relationships between every cyborg operating at a global scale – from individual hackers to the microprocessors in the Pentagon's computers – would require detail above and beyond the scope of this project. The breakdown between cyborg agencies is arguably endless, because human agency is not placed above that of inanimate objects – e.g., to study a particular hacker, one might need to include the grain the person eats for sustenance and, from there, the rain that goes into producing that very grain. (See Holloway, 2000, for an example of the intricacies involved in using this form of analysis). The lens of co-evolution allows for the critical analysis of economic and political flows between the real and virtual worlds, and thus, the mobility of power in the virtual can be correlated to real world conflict and vice-versa.

## Competing Geographies: Reflexive Modernization and Sub-politics in Cyberspace

The nodal network of cyberspace is a contested space. Though some have argued that ephemeral online agents hold an upper hand in these political conflicts due to their mobility, others argue that states have been, and will continue to, reflexively modernize to this systemic conflict between geographies – the nodal and the polygonic (Loader, 1997). Arquilla and Ronfeldt (2001b, 2001c) believe that both sides are right, postulating that it is only a matter of time before states adapt to network organization, because in the meanwhile non-state agents (e.g., Islamic terrorists, hacktivists) already embracing network organization maintain a distinct advantage in conflicts.

Everard (2000) argues that not only are “virtual states” a coming reality, humans have been functioning and organizing in them since the beginning of the capitalist world-economy. The state is a social construction, a fiction that dominates our lives (Everard, 2000, p.152). He argues that states offer an identity people subscribe to in order to receive certain benefits and responsibilities lying in a social structure (Everard, 2000, p. 152). Recently, much academic dialogue concerning “virtual states” has emerged due to the change from a spaces of places to a spaces of flows that network society is forging (Anderson, 2001; Castells, 2000; Everard, 2000; Rosecrance, 1996; Wriston, 1997). However, the state’s primary function in the world-economy – to provide an area of regulated production, trade, and finance for a sovereign market – should not be overlooked. Cyberspace acts as an extra-territorial institution for the U.S. and impedes on other states’ abilities to maintain this primary function.

Perhaps Luke provides the most thorough view of cyberspace’s network geography in his work on the geopolitical implications of the Internet. He contends that “in cyberspace ‘Real Life’ time warps and ‘Virtual Life’ space distorts leaving … virtual spaces that human beings must traverse” (Luke, 1998, p. 279). The key word here is “traverse,” signifying a flow of human agency across digital space. Time, as an element in the friction of distance, simply ceases to exist as a factor in virtual space, but direction remains and is distorted within the virtual world, as agents must navigate through a quagmire of nodes and connections. This cyber-network provides multiple paths to the same outcomes, making control over flows increasingly difficult for traditional political institutions based on territory and posing numerous risks for states (Arquilla & Ronfeldt, 1996, p. 79).

As aforementioned, at times in the past, space was seen as a collection of places. Though often it has largely been viewed as territorially based, today concepts of place are being forced to evolve into virtual reality as well. As Kitchin argues, what is of interest with the concept of cyber-place is that it is entirely a product of social processes, constructed from cyborgian interaction and having absolutely no physical aspects (Kitchin, 1998, p. 394). Though operating through silicon chips and fiber-optic wires, cyber-place is entirely imagined through digital communication. Currently, neither economic nor political aspects of state sovereignty extend efficiently into the networked virtual world – the place of virtual agency – which as will be discussed, is not only inducing the need for rapid reflexivity on the behalf of states, but is concurrently facilitating the rapid development of sub-political movements in civil society at large (Beck, 1992; Lenk, 1997; O'Tuathail, 1998).

Rheingold (1995, 2000) is perhaps the largest proponent of cyberspace acting as a place –a virtual community. He and others argue that public space is disappearing in the real world (Bauman, 1999), and therefore it is only natural that people use cyberspace as a new realm in which to act as a community (Castells, 2000; Kitchin, 1998, p. 396; Mitchell, 1999; Rheingold, 1995, 2000). Cyberspace allows communities to develop without a need for locale. Rather than being limited in personal networking by issues of proximity and adjacency, like-minded persons can form communities in cyberspace based on factors such as personal interests, morality, and common beliefs (Kitchin, 1998; Rheingold, 1995). Burrows (1997, p. 44) notes that “new global citizens wired up to the Internet … are busily forming new patterns of sociality, new virtual communities and thus new bases of power.” The view that power can form around certain online interests has gained much support by other theorists, and works in conjunction with Beck’s theory on sub-politics (Arquilla & Ronfeldt, 2001b, 2001c; Beck, 1992; Burrows, 1997; Froehling, 1997; Lenk, 1997; Loader, 1997, p. 8-9; Marden, 1997; Rheingold, 1995, 2000; Valeri, 2000; Wellman, 2001; Youngs, 1999).

Kitchin’s (1998) hypothesis, that cyberspace veneers a connected layer of nodes overlapping geographic space, holds dire implications for contemporary concepts of state sovereignty. Using this visualization of both the interconnectedness between the cyber and real world, the key issue facing the state system, and more specifically the U.S. as declining hegemonic power, is that the cyber-spatial world is a rhizome of infinite flows and connections to both itself and the territorial world. In contrast, real-world space is divided into a mosaic of bounded political entities based on territory and having but minimal influence extending into cyberspace.

By looking at Hudson's prerequisites for state sovereignty, it becomes apparent that the state system is ill prepared to extend its constitutive control into the Net. Luke boldly claims that due to the diverse and divided number of states in the world-economy, no single sovereign power will ever be able to encompass hegemonic power over all of cyberspace; the enforcement of national or supranational standards in the virtual world is impossible (1998, p. 281). However, Luke's popular speculation may prove to be incorrect. For as was noted in the previous chapter, the United States shares a distinct advantage in shaping international opinion around its policies and regulations due to prime modernity. Thus, the possibility exists that the inter-state system will conform around U.S. policies regarding the Internet, no matter the policies' effectiveness, and hence, give sway to U.S. hegemonic power in cyberspace (Lessig, 2001, p. 64-65). However, due to its position in the hegemonic cycle, that of decline, inter-state competition may prevent this from happening. No matter the eventual outcome, it is apparent that states are reflexively modernizing as political institutions to deal with the Internet.

Lack of systemic control of the Internet by any single state institution has led to an increase in the amount of international attention devoted to it. In recent years, the United States government has repeatedly addressed aspects of cyberspatial security and the need to establish dominance in the information industries (Auerbach & Bulkeley, 2000; Messmer, 2000; Neeley, 2000; Newman, 2000). The European Union took measures to foster quick extradition of people wanted for cyber-crime and is offering to extend the treaty to states around the world (Ward, 2001). Control over cyberspace has traditionally been sought through national court systems, but this method of enforcement has come to be viewed as largely ineffective; for, state-law is entwined with territorial aspects of place (rules governing behavior in communities within borders), and is thus rendered ineffective in a global network setting (Everard, 2000; Loader, 1997; Rosecrance, 1996). However, if current U.S. policy is to extend into the future, the recent anti-terrorism bill may open the way for United States extra-territoriality in states harboring electronic "terrorists" (CNN, 2001; Koch, 2001). The U.S. has begun to reflexively modernize its political and economic institutions. The conflict between this modernization of the traditional nation-state – as the political institution of production in the world-economy – and the resulting forms of sub-politics is being played out in cyberspace.

## Territorial Conflict in a Nodal World

As discussed in the last chapter, most world-systems theorists argue that U.S. hegemony is at the end of its hegemonic cycle – ushering in a period of systemic chaos. Silver and Slater view hegemonic transitions as moments of "escalating social conflict aimed at reaffirming or challenging established status and class hierarchies" (Silver & Slater, 1999, p. 211). Transitions are the product of intra-elite conflict, of which social unrest from peripheral classes is a byproduct (Arrighi & Sliver, 1999, p. 152). "The effects of financialization and polarization have been felt throughout the world capitalist system" with the result being both domestic and international disparities in wealth, which Silver and Slater link to growing racism and extreme nationalism, i.e., sub-politics and anti-systemic movements around the world (Silver & Slater, 1999, p. 213).

Many anti-systemic movements arise from issues over disparity in wealth, and thus, the continued exportation of the prime modernity of the American Dream, though helping the U.S. accumulate more capital, actually threatens the very stability upon which U.S. hegemony and the capitalist world-system depend (Taylor, 1996). Taylor argues that "Americanization" is a fallacy for all but the core in the world-economy, and it is inducing social conflict on a scale never before seen (1993, p. 19). There simply are not enough resources in the world for everyone to modernize or for an American standard of living to be universalized (Taylor, 1993, p. 19). There is growing opposition to globalization and American modernity, and as economic polarity increases, and the American Dream loses any semblance of universality, it can be expected that opposition from the peripheralized might become more confrontational and violent.

Unlike past anti-systemic movements, the opposition against the American modernity of mass consumerism is truly global in its scope. Furthermore, many risks have become associated with this American prime modernity (e.g., pollution, consumer waste, nuclear accidents, et cetera), which has triggered the concurrent growth of numerous sub-politics operating at the same time as anti-systemic movements. Most interestingly, the anti-systemic agents and sub-politics confronting U.S. prime modernity rarely associate themselves with any particular territorial entity (Arquilla & Ronfeldt, 1999a, 2001b). They are not protesting state abuses but rather trans-national transgressions. These anti-systemic agents and sub-politics are a manifestation of two things: the instability that hegemonic decline is bringing and the shifting metageography.

As already noted, anti-systemic movements' and sub-politics scale of conflict is enhanced by the rise of nodal communication technologies, which in many cases double hegemonic extraterritoriality back on itself by providing unimpeded avenues of penetration to non-hegemonic agents. As Andrew Ross writes: "The significance of these [online] cultures lies in their embryonic and protopolitical languages and technologies of opposition to dominant or parent systems of rules" (Ross, 1991, p.122). Even though they lack an overarching cause, all electronic civil disobedience moves toward questioning, and even unwittingly attacking, authority structures – particularly those based on territoriality. Thus, electronic agency presents a new medium through which sub-politics can arise, ironically utilizing a technological innovation of the hegemonic cycle and turning it into a double-edged sword for U.S. government institutions.

The use of this technological innovation to pressure institutions of political authority foreshadows the fact that cyberspace is likely to be increasingly utilized in all real world political conflicts (Arquilla & Ronfeldt, 1999a, 1999b, 1999c, 2001a, 2001b; Loader, 1997). Because of this, many argue that new social movements can emerge online that are not based on territorial or class identities like in the past, but on ephemeral social issues or narratives (Arquilla & Ronfeldt, 2001b). Essentially, they argue that Beck's sub-politics can form online in opposition to the reflexively modernizing state

(Himanen et al., 2001; Loader, 1997, p. 8-9; Poster, 1995, p. 87-90; Rheingold, 2000; Wellman, 2001). Globalization, while fostering a new network social structure and diminishing the power of state sovereignty, has also facilitated individual political sovereignty within the capitalist world-economy (Bauman, 1999, p. 4-7). Within the network society that globalization has begun ushering in, cyberspace has developed to house and support intermittent and broadly scaled networked communities that associate themselves around other forms of identity than the state (Wellman, 2001, p. 2031).

The technological development of cyberspace is not only bringing about the demise of state monopoly on political power to be shared with corporate trans-nationals, it is offering an opportunity for individual consumers and capital accumulators to partake in world politics on a global scale (Himanen et al., 2001; Stallabrass, 1995; Wray, 1998a, 1998b; Youngs, 1999). Moreover, virtual space provides a geographic arena for individual or group agencies opposed to both the declining United States hegemony and to the rising corporate ultra-hegemony, to engage in anti-systemic warfare in a non-territorial, ephemeral framework of linked nodes (Himanen et al., 2001; Loader, 1997; Wray, 1998a, 1998b).

## Nomadic Power and the Political Mobilization of Cyberspace

Thus far this chapter has reviewed various aspects of why states must attempt to establish regulatory control over cyberspace, likely under the leadership of U.S. hegemony. This analysis was done paying particular attention to the potential impacts online anti-systemic movements and sub-politics have on U.S. hegemony and the world-economy in general. Thus, before analyzing the conflict between sub-political movements and reflexive states in the coming network society, it is time to explain from where the potential energy of online politics stems and the different forms such agencies have begun take.

To be fair, aside from several celebrated attempts, mass-coordinated cyber-agency has not been astoundingly successful (Neeley, 2000; Wray, 1998a; Wriston, 1997). However, dissident groups are now capable of diffusing their beliefs, operations, and organizational structures cheaply and in a fashion that is difficult for governments to prevent or silence (Chroust, 2000; Everard, 2000, p. 158). This section will briefly catalogue the various techniques of cyber-resistance frequently encountered by states and corporations, but without offering any particular case study, which will be forthcoming in Chapter Five. Most online political organizations exist in the real world before they congregate in virtual reality (Auerbach & Bulkeley, 2000; Chroust, 2000; Hartigan, 1999; Sterling, 1993; Wray, 1998a, 1998b). However, as will be shown, this is not always the case (LoBaido, 1999; Sterling, 1993). For this thesis's analysis, political agents in cyberspace can be divided into two broad categories: 1) *real world political organizations*; and 2) *hackers*.

## Anti-systemic Movements and Organized Sub-politics in Cyberspace

Established political organizations as varied as Green Peace and the neo-Nazis have modernized and diffused into cyberspace (Whine, 1999). Already well established in the real world, such political groups make use of cyberspace to enhance various realms of their agency, including: recruitment, training, communication amongst members, and communication to the masses (Chroust, 2000) – the latter usually being laced with a particular propagandizing slant. These online movements are political institutions of the world-economy but, unlike states and many social movements throughout history (Taylor, 1991), they do not limit the scope of their conflict to the territorial confines of the real world.

The Chiapas movement in Mexico provides a well-documented example of how the Internet can be used by a real world political organization to successfully enhance its power against a state institution and expand the scope of conflict above and beyond state control (Froehling, 1997). It also demonstrates the triviality of traditional state methods of political regulation and control in the dawn of the network society. Still maintaining full sovereignty and the right to use violence, Mexico has repeatedly failed to quell Chiapas resistance and has incurred the wrath of an international networked community of Chiapas supporters (Ronfeldt, Arquilla, Fuller, & Fuller, 1998). The power of Chiapas online resistance comes from the networked geography of the Internet. Supporters can arrive at various crucial nodes within Mexico without ever having to cross a territorial border (e.g., logging into the Mexican Government's intranet from a home computer in the Philippines).

Varying drastically from standard approaches to utilizing the Internet, *hacktivism* provides certain online agencies various evolving methods of organizing political action across the medium of the Internet. Self-ascribed "hacktivist" groups are often representations of sub-politics in cyberspace. Though these groups do not necessarily exist in the real world – there is rarely any hierarchical organization to them – they express and maintain ephemeral identities molded around common interests above and beyond territorial or traditional ideological affiliations (e.g., environmental activism). Hacktivist organizations use cyberspace as their field of operations against real world adversaries. Arguably, hacktivism may pose the largest organized challenge to U.S. hegemonic attempts to control cyberspace.

Wray (1998a, 1998b) has been one of the largest academic proponents of hacktivism, and has written extensively on the philosophies behind electronic civil disobedience. He argues that the strength of hacktivism is that it is capable of mobilizing people in a virtual environment rather than territorially (1998a). The network geography of cyberspace provides a virtual realm in which a social movement can recruit, organize, mobilize, and transitorily unite to concentrate their efforts on the disruption of government and corporate functions (Cassel, 2000; Goldberg, 1999; Hartigan, 1999; Poster, 1995, p. 81-84; Radcliff, 2000; Wray, 1998a, 1998b). For example, the logistics behind gathering 100,000 persons from around the world to have a sit-in at the White House in Washington, D.C., would be difficult. Moreover, authorities would most likely attempt to thwart such a protest through regulation and police barricades. However, a hacktivist organization may coordinate a similar protest with an equivalent amount of online agents logging onto the Internet and flooding the White House's communications network. Coordinated denial of service attacks effectively cripple electronic communication (Wray, 1998a, 1998b).

Arquilla and Ronfeldt (1999a, p. 53; 1999c, p.198) have labeled such pulsing, choreographed, and overwhelming network attacks as “swarming.” Swarming “occurs when the dispersed nodes of a network of small (and perhaps some large) forces can converge on a target from multiple directions” concurrently (Arquilla & Ronfeldt, 1999a, p. 53; 1999c, p. 198; 2001b, 2001c). Swarm networks are able to coalesce quickly on a target without prior warning and disappear just as quickly without any central place to counterattack. Due to its effusiveness and brief temporality, swarming jeopardizes the effectiveness of traditional forms of defense based on territorial and hierarchal organization, which has dire implications for the most interconnected state in the world – the United States (Arquilla & Ronfeldt, 1999a, p. 53-55; 1999c, p. 198; 2001b).

Studies of ephemeral aspects of political agency have existed in the geographic discipline for some time. Perhaps most pronouncedly, Warf and Grimes describe such potential for counter-hegemonic action as “nomadic power” (Warf & Grimes, 1997, p. 269). Nomadic power is defined as diffuse, without territorial location, and remains autonomous through movement (Warf & Grimes, 1997, p. 269). Traditional control of economic processes by the elites, or core agents of the world-economy, can be resisted by nomadic forms of power through electronic mediums.

Once again, the development of this new form of political agency stems from the dynamics of the capitalist world-economy. As the world-economy is in the B-phase of the Kondratieff wave and at the end of the hegemonic cycle, production is evolving in the core, and old forms of production are shifting to the periphery. The valuables of nomadic power are those of developed, or core, capitalism – electronic information and knowledge. These valuables are not tangible, and by virtue are located nowhere in the real world, yet are potentially accessible from everywhere in cyberspace (Warf & Grimes, 1997). “Nomadic Power cannot be physically captured,” as it is not territorially based (Warf & Grimes, 1997, p. 269). As the state has traditionally been the producer and protector of valuables, it finds its territorial basis for the regulation of flows has become insufficient for the security of core capitalism’s digital capital (Mitchell, 1999).

It is due to the diffusion of power away from territorially based political institutions (i.e., the state) that hacktivism and online agency becomes an applicable method of resistance against hegemony and the world-system in general. As Beck (1992) argued, this diffusion of power to sub-politics is common during times of reflexive modernization. Due to its establishment as an open and free network, very few checkpoints are in place to keep social movements from hopping on the Internet and trespassing upon every state's sovereignty. As the U.S. has more portals than any other state, and lies at the heart of many sub-politics' agenda, it stands to be transgressed and attacked the most.

As will be the focus of the next chapter, hacktivism offers a dichotomous perspective from that of the nation-state in regards to the spatiality of cyber-warfare and online political agency. The classic state-centric approach to defining information warfare is epitomized in Gray's perspective of cyber-war as "the offensive and defensive use of information and information systems to exploit, corrupt, or destroy an adversary's information and information systems, while protecting one's own" (Gray, 1999, p. 268). Gray makes little or no mention of independent actors outside of other state adversaries. Because of this, he proposes that "electronic combat can be considered within the same intellectual framework that rules the relevant geographies for land, sea, air, and space warriors"; though, he is forced to admit, unlike in other geographic realms, virtual warfare "cannot bear the traffic of war with 'bombs and bullets'" (Gray, 1999, p. 268). Online proponents, such as Wray, have taken a more explicit approach to categorizing telecommunications warfare than most state policy makers.

Wray subdivides virtual warfare into two types: cyberwar and infowar (Wray, 1998a, 1998b). *Cyberwar* exists when any side in a conflict is dependent upon computers, e.g., the United States Armed Forces with their high-tech cruise missiles (Wray, 1998a, p. 4), or more manifestly, when dependence on high technology allows enemies to avoid attacking power bases in the real world and instead launch attacks against electronic systems (Wray, 1998a, 1998b). The other type of resistance embraced by hacktivism is *infowar,* which is a war of propaganda and rhetoric. The Internet medium offers not only the most cost effective method of information dissemination, but also the largest scale of potential audience (Warf & Grimes, 1997). For peripheral regions and peoples of the world, the Internet provides one of the few methods through which to circumvent state or media controls over information. However, when hacktivism fails to achieve desired goals, another method of protesting state or hegemonic control is to personally attack the political institution itself – anonymously.

## Hackers: A Case of Maladaptive Cyborgs

The definition of a "hacker" is still heavily debated and constantly undergoing reformation, but since the earliest days, definitions have all concurred that hacking involves an individual using telecommunications tools and a computer to gain access to information that one would otherwise be unable, or unauthorized, to obtain (Balsamo, 1995; Hacktivist.com, 2001; Hafner & Markoff, 1995; Poster, 1995; Sterling, 1993). The term first originated in the 1950s and referred to computer engineers at MIT who "hacked" in order to get the primitive computers to work – "an unorthodox, yet talented, professional programmer" (Hacktivist.com, 2001, p. 2).

In 1983 the movie *War Games* helped usher in the definition of hacker that continues to predominate today – one who obtains access to computer networks either illegally or via unauthorized procedures (Hacktivist.com, 2001). However, definitions still vary upon perspective. Social scientists have been particularly loath to circle around an objective definition of hacker, often obscuring definitions behind terminology such as "electronic trespassers" and "digital vandals." Hackers have an even more difficult time expressing their own identity – that of crusaders in a battle for free information – as their views are constantly overshadowed by the media expressing hacker identity for them – maladaptive rogues that are a risk to society at large (Clark, 1995, p. 118; Hacktivist.com, 2001; Himanen et al., 2001).

Hackers are primarily known for breaking into well-protected intranets often for the sheer joy of it (Hacktivist.com, 2001; Sterling, 1993). Sometimes successful hackers do nothing to "owned" data; other times they disseminate the information they have obtained to the public, and frequently, they steal whatever information they have uncovered and disappear (Sterling, 1993, p. 50-59). Until recently, governments around the world had relatively light laws on hacking, but this has changed, as online attacks have become more brazen, economically motivated, and more politically based (Anonymous, 2000; Schwartz, 2000; Wray, 1998a). Potentially more dangerous still for U.S. security, is the development of hacker terrorist groups. The U.S. Government has previously stated its apprehensions about hackers working together through cell groups and posing a real threat to U.S. security as they have in the past to particular corporations and the People's Republic of China (Auerbach & Bulkeley, 2000; Cassel, 2000; Freedman & Mann, 1997; Goldberg, 1999; Hafner & Markoff, 1995; Koerner, 2000; LoBaido, 1999; Newman, 2000; Price, 2000; Radcliff, 2000; RIA, 2000; Sterling, 1993).

Definitions and societal fears aside, what is distinct about hackers and movements that utilize hacker techniques is their ability to conduct protest and warfare quietly and, most often, without detection (Ross, 1991, p. 120-121). Power without checks and balances and lacking recourse to identify those bearing responsibility is a risk to civil society (Sterling, 1993, p. 51). Stemming from society's fear of this risk, U.S. prime modernity has constructed the use of technology for political action as being deviant (Hacktivist.com, 2001; Poster, 1995; Ross, 1991; Sterling, 1993). Ross argues that like the hippies of the 60s and the punks of the 70s, today's hacker "has come to serve as a visible public example of moral maladjustment, a hegemonic test case for redefining the dominant ethics in an advanced technocratic society" (1991, p. 119). In complete juxtaposition to the identity of hackers espoused by U.S. hegemony and the media, in reality the hacker underground is dominated by a technological elite (Sterling, 1993; Stone, 1995) with the self-understanding that "they are the apprentice architects of a future dominated by knowledge, expertise, and 'smartness,' whether human or digital" (Ross, 1991, p. 121). The increase in computing seen over the past 20 years has mutated attitudes toward technology in various ways (Fitting, 1991, p. 302). In contrast to those who remain phobic of computers, hackers view new technology as a means of liberation (Fitting, 1991, p. 302).

For all intents and purposes, the U.S. has a good reason to wage propaganda war against hackers. For if Castells and Himanen (2001) are to be believed, hackers represent an entirely new form of socialization for the new network metageography – one that threatens the ethics underlying the capitalist world-economy since its inception. As the most valuable capital in the world-system increasingly continues to become information and knowledge, the network geography of cyberspace is a subterfuge to protection of such properties. The "hacker ethic," evolving under contemporary informationalism and the evolution to network society, may very well threaten notions of property ownership upon which the capitalist world-system depends (Himanen et al., 2001).

## The Socialization of the Virtual Network

In essence, the hacker work ethic stems from curiosity. Linus Torvalds, inventor of the Linux operating system, argues that progress is about channeling human agency through three phases of evolution: survival, social life, and entertainment (Himanen et al., 2001). He believes that capital accumulation is not necessarily the motivation behind human agency, but that it is merely "motivational for what it brings – it's the ultimate bartering tool for things we really care about" (Himanen et al., 2001, xv). However, whereas it is relatively easy to achieve the first phase of survival, for those not included in core processes "it is much more difficult to buy social ties and entertainment" (Himanen et al., 2001, xvi). A hacker, Torvalds argues, "is a person who has gone past using his computer for survival to the next two stages" – for establishing social ties and entertaining oneself (Himanen et al., 2001, xvii).

Himanen (et al., 2001) takes Torvald's concept of "entertainment" yet further, viewing hackers' "passion" for work as all pervasive and a real threat to the Protestant work ethic of the capitalist world-economy. He argues: "Computer hackers can be understood as an excellent example of a more general work ethic gaining ground in our network society, in which the role of information professionals is expanding" (Himanen, 2001, p. 7). He goes on to postulate that the reason "hackerism" is considered so radical and vilified around the world today is because it is "proposing an alternative spirit for the network society – a spirit that finally questions the dominant Protestant ethic" of working to work (Himanen et al., 2001, p. 12-13). Himanen (2001) counterpoises the Protestant ethic with hacker ethic by tying each to two contradictory philosophies – monastic and academic, respectively. The monastic roots of capitalist society are based around information control, working for the sake of work, and rigid time control (Himanen et al., 2001). In contrast, the academic roots of network society are about information sharing and diffusion, working for causes of self-determined value, and unstructured time – money is not so much a driving force as recognition and reputation are (Himanen et al., 2001).

The changes arising during this network revolution in perception toward work, capital, and property have dire implications for states. These territorial political institutions rely on the ceaseless accumulation of capital and property protection to maintain their power and position in the world-economy. Though they can reflexively modernize to the actual risks that they have themselves unleashed, reacting to societal changes in values stemming from these risks is obviously more troublesome. It is this new ethic that presents a platform for sub-politics in the cyber-network to coalesce around, and offers a bitter ideological rival to state institutions in the process of institutional adaptation – primarily the United States and its liberal agenda.

## States Versus Networks

Institutions of the capitalist world-economy developed by the inter-state system are currently in a quandary on how best to handle new politics based on the network society. Quite prominently, this is obvious in the U.S. hegemony's inability to deal with online sub-politics. However, risks stemming from the Net also include mundane ones found everyday throughout the real world. Though coded communication between terrorist cells has become a reality consuming public consciousness (Sieberg, 2001), perhaps a far greater delegitimization of the state is found in things such as online pornography, pedophilia, and monetary fraud. Most of these online dangers are not intentionally anti-systemic but nevertheless threaten state authority.

The hegemony has an inherent interest in expanding its institutional influence over the Internet. As cyberspace ushers in new forms of political power, a dilemma arises as to how the U.S. can reflexively modernize in order to regulate and police the virtual world (Lenk, 1997; Loader, 1997, p. 14). Traditional methods of control, rooted in territory, will not suffice, for electronic space overarches sovereign space (Sassen, 1996). In order to regulate electronic flows, states may need to reanalyze what has secured their dominating presence on the territorial landscape over the past four hundred years. Looking back at history, a logical choice for state actors is to recognize and legitimize one another's institutional sovereignty over some definable and demarcated type of virtual space (Mann, 1997).

Though the concept of mutual recognition of sovereignty is well dialogued, Brunn was the one of the first geographers to assert this idea toward cyberspace. Brunn (1999) argues that new communities are appearing in virtual space with interests in state political discourse, many residing outside of a state's regulatory boundaries. Thus, he concludes that modern-states need to ratify a treaty, or at least agree on a set of rules and regulations for the Internet (Brunn, 1999). Others, particularly those working in some capacity for the U.S. department of defense, agree (Arquilla & Ronfeldt, 1999b; Valeri, 2000). They argue that the major actors in the world economy, i.e., states with the most advanced telecommunications technologies and well organized interest groups (e.g., corporations), need to create an "international regime" (Valeri, 2000) in order to protect information and knowledge property within the world-economy (Brunn, 1999, p. 125). Traditionally, states sign treaties when they cannot agree on how best to resolve a conflict, and during this period of hegemonic decline, some argue it is imperative that states and powerful figures of the world-economy agree to some sort of "Treaty of Silicon" (Brunn, 1999; Valeri, 2000). If nothing else, a commitment to open coding, a reevaluation of outdated copyright laws, and standardization of the makeup of online content may be needed (Lessig, 2001). Lessig argues that innovation stemming from the Internet, through which the U.S. has profited heavily in recent years, is threatened by bad U.S. policy making (2001, p. 63-65).

Others argue oppositely, that standardization and the establishment of a virtual inter-state system is a misguided, if not impossible, delusion of grandeur. As Barlow notes: “Cyberspace is naturally anti-sovereign” (as cited by Luke, p. 281), and cyber groups must *defend* civil liberties against “hegemonic incursions by various power sources from the terrestrial world” – more commonly referred to as the state (Luke, 1998, p. 278). Further complicating Brunn’s call for a Treaty of Silicon is the assumption that all states would see benefit in such a treaty, particularly the U.S. hegemony. As geohistorical analysis demonstrates, the U.S. is unlikely to endorse any plan that alleviates its online hegemonic extra-territorial dominance in economics, politics, and culture. Moreover, any such form of reflexive modernization would not necessarily be easy or obvious for states to partake in. States will continue to conflict with one another over political policies affecting their populations – even if states agree on online regulation policy in principle (Everard, 2000, p. 115).

However, isolationism from the Internet is not an option for states unwilling to cooperate in a treaty, either. Everard notes that a majority of states are and will remain unwilling to cut themselves off from the global flows of information, as staying connected helps to maintain a semblance of virtual sovereignty (2000, p. 52). Thus, a state’s disposition to allow unregulated electronic information into its territory “becomes an issue of moral persuasion [on the part of the hegemony] such that access to the global information economy must be seen to have tangible benefits to the country that outweigh the risks of allowing dissent” (Everard, 2000, p. 52). Once the risks in global society at large increase to a point of unbearable proportions, current institutions will either need to evolve or new ones will emerge (Beck, 1992; O'Tuathail, 1998). Online non-profit organizations may represent such new institutions, and states might benefit by reaching out to cooperate with them rather than, as current U.S. policy often dictates, viewing them as potential adversaries in the geopolitical order (Arquilla & Ronfeldt, 1999b, p. 74-75; Valeri, 2000). Through analysis of the hegemony’s reactions to cyberspace, as it is the leader of the geopolitical order, potential trends in the political regulation and institutional modernization of cyberspace can be predicted.

### The Governance of Cyberspace

As Himanen (2001, p. 25) notes: “In the culture of speed, immobility is even worse than slowness.” In a society based upon unimpeded flows, any institution based on place and constancy will either need to redefine itself or become obsolete. As the U.S. has arguably gained more than other states from the diffusion of cyberspace around the world – through extra-territoriality – a self-induced problem has developed in that its extensive connections to the virtual world, as well as its role of representing the source of numerous risks because of its position as world hegemon, now cement the U.S. as a prime online target for sub-political uprisings (Swartz, 2001). Because of this untenable position, the U.S. will seek to modernize so that it can regulate cyberspace.

Loader (1997) argues that in order to understand state attempts to govern the Internet, one should look to Foucault. He believes that governance is meant to help citizens by protecting them and keeping them well off, and that in return, the citizens will support the governing body. Thus, governance in cyberspace implies that power relationships based upon identity and compliance will continue to be an important part of online human interaction (Loader, 1997, p. 15). However, this view of governance assumes that a territorial affiliation will transcend into the networks of virtual space – something that has not yet happened and that many argue cannot. As Arquilla and Ronfeldt note, the only way to fight an adversarial network is with a network (1996, 1999c, 2001a, 2001b, 2001c).

As Beck (1992) theorizes, there is no doubt that states are reflexively modernizing to the causalities of network society, but thus far, U.S. efforts to modernize against the risks of the Internet are hampered by a type of spatial dementia – approaching new policy making through the traditional perspective of territorial geopolitics. As world hegemon, the U.S. will lead development in establishing how the inter-state system contends to regulate the Internet, and it will most likely seek such changes through consensus. If consensus cannot be forged, reflexive modernization will no doubt include advancing cyberwarfare technologies – as has already begun (CNN, 2000; Messmer, 2000; Wray, 1998b).

Burrows espouses that any mention of state governance in virtual space is “in actuality an implicit device for beginning the task of conceptualizing the exhaustion of the nation-state” (Burrows, 1997, p. 44). Stating that cyberpunk literature provides us with the reality of the world today displaced in a future setting, he suggests that the state is being overtaken by supranational cultural and political formations – reflexive modernizations away from the traditional state (Burrows, 1997, p. 44). Governance is still founded on the capitalist world-system and around the ceaseless accumulation of capital, but the state has begun withering to just another service industry (Burrows, 1997, p. 44).

In contrast, Castells and Everard concur that states will not disappear in a network society but, rather, they will continually “adapt in structure and performance, becoming networks themselves” (Everard, 2000, p. 115; Himanen et al., 2001, p. 171). The simultaneity of power being shifted both upward and downward is creating the “network state,” which will remain as the most resilient institutional form in the network society (Everard, 2000, p. 115; Himanen et al., 2001, p. 172). Castells goes on to note that the proliferation of transnational businesses is the driving impetus behind the informationalism paradigm, the network society, and is pushing the evolution of the state (Himanen et al., 2001). During the height of U.S. hegemony, numerous startup businesses quickly became gargantuan by exporting themselves trans-nationally. These businesses were established and grew on the technological innovation of hacker culture and individual inventors (Himanen et al., 2001, p. 177; Lessig, 2001, p. 61). Though financing, production, and trade determine which technologies survive in the marketplace, they do not necessarily influence which technologies continue to develop (Himanen et al., 2001, p. 177). This is determined through cultural revolutions, which fuel the processes behind technological paradigms. Castells believes the revolution behind informationalism began in the 1960s and continues to manifest itself in the hacker ethic that is guiding society toward network organization (Himanen et al., 2001, p. 172-177).

The Internet is ripe for use by sub-politics during this time of hegemonic decline and reflexive modernization. For, even though the Internet began as a technological innovation of U.S. hegemony, it has been developed by social movements, and therefore, currently lacks state input and safeguards in security and regulation. Until the early 1990s, the Internet's commercially exploitable properties went unnoticed, and its properties were shaped by hackers and academics. It developed as a means of communication between the new social movements, a method of easy data liberation and diffusion. With corporate expansion into the virtual world and the Internet's subsequent globalization, a dichotomous battle of ethics has ensued – capitalist world-economy (control, regulation, and exploitation for profit) versus the sub-politics of the hacker ethic (free and open access to, and diffusion of, information, regardless of content). It is a contemporary battle over the commons (Lessig, 2001, p. 58), but quite unlike the local repercussions of such past conflicts, this time it is occurring on a global scale.

## Conclusion

Cyber-spatial resistance presents a real challenge to hegemony and state sovereignty in the 21st Century. Traditional methods of territorial control associated with the state institution do not permeate well into the socially constructed, virtual network space. The state's role in the world economy is currently changing, and lack of hegemonic control in cyberspace leaves open a frontier of access to the state institution through which any human agent can enter. This is particularly true for the United States, which was the site of the Internet's origin and is more connected, hence susceptible, to the politics of the virtual world than any other state. The growth of online sub-politics around the risks of U.S. prime modernity has the potential to undermine the world-economy by delegitimizing the current hegemonic order and by rendering traditional institutional concepts (e.g., state sovereignty) on which hegemony functions, essentially useless. Moreover, by thwarting the attempts of core agents to control the flows of valuable knowledge and information, the ceaseless accumulation of capital (formerly tangible goods) on which the capitalist world-economy depends is threatened by a ceaseless diffusion of capital (today digital knowledge and information), which may push the system into crisis.  As world leader, the hegemony will attempt to use its power to maintain such control in the world-system.

The most noticeable dichotomy between these two adversarial forces is that of geography.  Virtual movements are grounded on territorial principles, yet they utilize the nodal network of cyberspace and the opportunities that such a geographic structure offers.  The U.S. thus far has insisted on confronting virtual conflict with the same strategies and tactics used in territorial geopolitics.  This clash in approach and perspectives between the new social movements and the hegemonic power has dire implications for the future of the world-system.  It represents a larger, more pronounced conflict between spatial ideologies: that of territorially defined place (i.e., control and regulation through borders) versus that of networked flows (i.e., ephemeral, dynamic power diffusion).  If the hegemony's ability to regulate and maintain order is thwarted, the system may be thrown into crisis.  However, policies currently being penned are trying to avoid this.

Policy is for governments to make and for revolutionaries to break.  By analyzing U.S. policy makers' perceptions regarding conflict via networks, and in turn comparing and contrasting it with the viewpoint of online sub-politics and anti-systemic movements, we will better be able to understand this ideological battle over the virtual commons.  In the following chapter, we will critically analyze documents of the ANSER Corporation's Office for Homeland Security and the RAND Corporation – two federally funded think-tanks that shape and make U.S. policy in regards to netwar.  It is in these documents that it becomes apparent that the ideological dichotomy between U.S. hegemony and online sub-politics is really a conflict of changing geography.

## Chapter Four: Hegemonic Attempts at Reflexive Modernization

The U.S. as world hegemon has a vested interest in keeping the Internet open for global trade, finance, and communication.  Not only does cyberspace facilitate American extra-territoriality through the exportation of predominantly American cultural artifacts (Holloway and Valentine, 2001), but it has also become an incredible tool for the accumulation of surplus capital and the maintenance of economic dominance .  However, in contrast to the benefits provided to the declining hegemon, cyberspace also presents numerous problems for national security – providing innumerable avenues of attack on the United States, its institutions, and its critical infrastructures.

During periods of hegemonic decline, challenges against the world hegemony and the geopolitical order through which it maintains its power become more frequent (Modelski, 1987).  The network geography of the Internet has instigated the deterritorialization of the current geopolitical order.  In turn, this deterritorialization has invited new political agencies, other than nation-states and territorially affiliated political organizations, to the realm of international politics and action, and as might be predicted, quite often these new actors target the contemporary center of power in the world-economy – the world hegemony.  As the United States struggles to reflexively modernize to the newest and most dangerous security risk since the advent of nuclear weapons (Beck, 1992), it finds its policies and techniques for securing power both ineffective and obsolete – tainted by territorial assumptions and hierarchical procedures that have no place in the network geography of cyberspace (Agnew, 1994, 1998).

Through analysis of U.S. "national security" and "homeland defense" policy in the virtual world, a few characteristics become apparent.  First, the United States is desperately attempting to reflexively modernize its defensive capabilities to alleviate the risk that inadvertently remains as a side-effect of a technological breakthrough – the proliferation of the Internet and networked telecommunications around the globe.  Second, thus far and for the foreseeable future, attempts to modernize Federal institutions to deal with the new security risks have been contradictory and disjointed.  Third, the fundamental reason behind the world hegemony's inability to resolve the above stated risk is that it suffers from a type of spatial dementia; a creature of habit, the U.S. continually attempts to modernize itself using territorial methods and policies that do not work in the network geography of cyberspace.

This chapter will review the spatial disjuncture between U.S. defense policy and the reality of cyber-conflict by critically analyzing documents produced by two of the primary not-for-profit corporations informing U.S. network defense policy – RAND and ANSER's Institute for Homeland Security. Through analysis of these two government-funded corporations' publications concerning homeland defense against network warfare, it will be shown that, when implementing modernization policies, U.S. national security suffers from an ignorance of the new spatiality behind online conflict. The chapter will be divided into three parts: 1) an overview of the power and influence that RAND and ANSER have in shaping U.S. defense policy; 2) a review of "risks" to U.S. security, as identified through ANSER and RAND publications, and the subsequent methods of reflexive modernization that RAND and ANSER experts have recommended to the U.S. government; and 3) contradictions between U.S. policy and online security stances and the realities of defending against new sub-politics in cyberspace.

## RAND and ANSER: Hidden Powers Behind Homeland Defense Policy

> "Mister President, under the authority granted me as Director of Weapons Research and Development, I commissioned a study of this project by the *BLAND* Corporation last year." – Dr. Strangelove, in *Dr. Strangelove: or How I Learned to Stop Worrying and Love the Bomb* (George, 1998, p. 108).

As the classic parody of nuclear holocaust, *Dr. Strangelove*, cynically makes note of (Brandenburger & Stein, unknown; Siano, unknown), the RAND Corporation has arguably become the most prominent and important technology and strategy developer for the Department of Defense since the Second World War. Its origins are firmly rooted in the military-industrial complex of the Cold War, breaking off from Douglas Aircraft Company in 1948, to become an independent, not-for-profit corporation helping guide

United States Air Force (USAF) development and strategy (Anonymous, 2002f). Free from the limitations of working solely for the defense industry, it quickly reorganized itself around a broader mission – to "promote scientific, educational, and charitable purposes, all for the public welfare and security of the United States of America" (Anonymous, 2002f).

Technology has always been at the center of the RAND Corporation's interests, involved in the early stages of Internet development. It was a RAND researcher who initially conceptualized "packet switching" – upon which the Internet came to depend and continues to function today (Baran, 1964). During its rise and growth, RAND also began to emphasize the development of "theories and tools for decision-making under uncertainty," contributing to the development of game theory, dynamic programming, mathematical modeling, and *network* theory (Anonymous, 2002f). Today, RAND has spawned off other not-for-profit corporations, maintains its own graduate school in Santa Monica, California, and holds as its "primary function … research on complex policy and problems where multidisciplinary capability, objectivity, and an explicit national-interest charter are essential" (Anonymous, 2002d).

Cyberwar and the protection of critical infrastructures connected to the Net are two prime examples where multidisciplinary interests and national-security needs cross, and RAND has been at the forefront of publishing policy, strategy, and technological solutions to the emerging and contemporary threats of the networks fueling globalization – what RAND researchers term "Noopolitik" (2002d; Arquilla & Ronfeldt, 1999b). In the last ten years, RAND has conducted studies, role-played information war scenarios for the Department of Defense (Molander, Riddile, & Wilson, 1996), published numerous documents pertaining to, and recommending strategies for, Federal policy to thwart and defend against information war (Arquilla & Ronfeldt, 1996, 1999a, 1999b, 1999c, 2001a, 2001b, 2001c; Buchan, 1996; Molander et al., 1996; Ronfeldt, Arquilla, Fuller, & Fuller, 1998; Ware, 1997), and has profoundly influenced the policies promoted by the recently appointed head of U.S. Cyber-Security, Richard Clarke (Lemos, 2001; Vaida, 2001).

Perhaps more influentially, however, throughout the years various sections of RAND have branched off, becoming independent entities specializing in particular areas of policy development. Though RAND stands at the forefront of researching and evaluating network and cyber-defense for the U.S. government, it is one of RAND's offshoots that has become the primary disseminator and informer of homeland defense policy, including cyber-security.

> "ANSER's driving objective is to make a difference—that is, to help our nation's public institutions cope with current and emerging challenges. Our product is the intellectual output of our people. Our goals are to steadily increase our impact on national priorities…" – Dr. Ruth David, CEO (Anonymous, 1999).

Established in 1958 as an offshoot of the RAND Corporation, ANSER has evolved over the past 43 years from an independent, not-for-profit corporation limited to conducting "unbiased studies and analyses" (Anonymous, 2002a) for the USAF to a company that is primarily concerned with helping to "[s]trengthen public institutions" through "the improv[ement] of their effectiveness and efficiency" (Anonymous, 2002b). As its prowess in helping government institutions modernize and keep up with changing technology and threats has grown, so too has its budget and personnel – to a company of over 700 employees and a budget exceeding $70 million at the turn of the millennium (Anonymous, 2002a).

With an increasing budget and staff, in the 1980s ANSER's prime role began to evolve and become more concrete: to "[h]elp protect U.S. technological leadership by nurturing the science and technology workforce" (Anonymous, 2002b). Tucked at the end of its corporate mission, ANSER states that it hopes to contribute and influence U.S. government dialog and subsequent policy on particular "critical and transnational issues" (Anonymous, 2002b). The CEO, Dr. Ruth David, defined ANSER's role in forging policy even more explicitly in the 1999 Annual Report, noting that ANSER is shifting its focus to two specific realms of policy making, the primary one of which is homeland defense (Anonymous, 1999). Hence in 2000, ANSER developed the *Institute for Homeland Security*, a subsidiary component of the corporation concentrating on the production and dissemination of national security policy-making publications. Through the Institute, ANSER established a new journal, *The Journal of Homeland Security*, and weekly email newsletters providing up-to-date news and hypertext links to articles and documents concerning issues of defense policy. Since then, Federal awards, accolades, and continued contracting have proven that "ANSER's research staff has become a recognized source of articles, lectures, and commentary" on security and technology (Anonymous, 1999).

Less than two years old, the Institute has already gained recognition outside of the Beltway as a landmine of information regarding timely and in-depth debates concerning national security policy. The Institute's newsletter provides one example of ANSER's increasing position of influence, as initially fewer than 100 people subscribed to the weekly email, which has now grown to include over 10,000 readers (Anonymous, 2002c). The Institute's *Journal of Homeland Security* is quickly becoming a staple for those involved in national security industries, as it provides a comprehensive overview of homeland defense, with article authorship being balanced between defense experts and academics alike. Due to its rising influence, earlier this year *Foreign Affairs* published a review of the Institute for Homeland Security, noting that the Institute's "Web site presents an array of resources, including an online journal, access to the syllabi of several courses on terrorism and homeland security, links to a wide array of Internet sources, and a large virtual library" on homeland defense (Cohen, 2002). Furthermore, the review praised the Institute's "partnership agreements" with other policy-oriented agencies such as the Center for Strategic and International Studies (CSIS) and the RAND Corporation (Cohen, 2002). The Secretary of the United States Air Force hailed ANSER for producing products for the defense industry "marked by quality, responsiveness, and objectivity" (Sec. of USAF, as cited by ANSER, 2002b).

Due to its newly proscribed role in defense policy development, and coupled with its emphasis on technology, ANSER's Institute for Homeland Security – including its virtual library, weekly newsletters, and the *Journal of Homeland Security* – offers an excellent specimen to examine and gauge the processes of U.S. policy in cyber-spatial conflicts and defense. Furthermore, coupling analysis of ANSER's commentaries on U.S. cyber defense with those published by RAND, as well as those produced by affiliated partner agencies such as CSIS, will provide insight into the debates and the strategic direction behind current and forthcoming U.S. policy decisions. The rest of this chapter will critically analyze a plethora of documents that these government sponsored corporations have produced, or endorsed, pertaining to U.S. reflexive modernization and defense strategies to cope with the advent of network war, information war, and cyber-spatial conflict.

### Network Vulnerabilities: The Side-Effects of Cyberspatial Preeminence

Though some argue that the Internet presents the greatest risk to national security in contemporary times, policy makers agree that the U.S. must "understand that [the] benefits far outweigh any risks" (Cilluffo, 2000). As Cilluffo warns in the *Journal of Homeland Security*, however: "Along with the clear rewards [of America's dominance over the Internet] come new risks and a litany of unintended consequences that need to be better understood and managed by our industry and government leaders" (Cilluffo, 2000). As Buchan notes in a RAND publication analyzing the Air Force's cyber-defenses, "Vulnerability is the 'flipside' to the leverage that information offers" (Buchan, 1996). Thus, many argue that if the U.S. begins to better use its informational dominance, cyberspace may become a critical and paramount component to the successful maintenance of U.S. national security (Buchan, 1996; Molander et al., 1996; Stephenson, 2002).

No matter the threat of extremely disruptive cyber-attacks, consensus espouses that it is now impossible to shutdown the current infrastructure of the Internet and begin from scratch to build a new, more secure version of cyberspace (Molander et al., 1996, p. xvii). As a White Paper to President Bush from a government funded study group – available in the Institute for Homeland Security's library – espoused early in his term:

"Engineering practices and technology cannot produce systems that are totally immune to attack, but the risks can be reduced and made manageable" (Anonymous, 2001, p. 2). And as a book published by RAND for the U.S. Department of Defense has made clear to the government, security is not gained "simply [by doing the] opposite of the vulnerabilities" (Anderson, 1999, p. 48), and "[i]t is important to realize at the outset that technical constraints make it impossible or infeasible to eliminate certain vulnerabilities by straightforward redesign" (Anderson, 1999, p. 47).

Here to stay, the best U.S. policy can hope to do is help guide the Internet so that it evolves into something more secure and controllable, as "[t]he best way to predict the future is to help build it" (Cilluffo, 2000). In order for this to happen, it has been imperative for policy-makers to identify, label, and address the plethora of susceptibilities that the Internet offers adversaries to confront the world hegemon, as well as identify who the potential adversaries might be. Though variations in the definition of cyber vulnerabilities and defense challenges exist, four specific ones recur in ANSER, RAND, and other affiliated organizations' analyses (see for example: Anderson, 1999; Anonymous, 2001; Cilluffo, 2000; Lenk, 1997; Ware, 1997): 1) threat of an attack on U.S. critical infrastructures, including the interruption of communication and financial flows, as well as the disruption of public and political services and processes; 2) threat of the manipulation of sensitive or classified information for political, economic, or military purposes; 3) difficulty in deciphering malicious activity from "background noise" (i.e., everyday software glitches and networking problems); and 4) information assurance on networks in the private sector. These four themes have dominated risk assessment studies by U.S. policy-makers, and demonstrate that, strategists at least, understand the crucial role of information technology in the United States' position of world power.

One facet of the information revolution is at the center of all the risks associated with cyberspace – the blurring of certain institutional boundaries upon which the U.S. has come to maintain its power (de Borchgrave, Cilluffo, Cardash, & Ledgerwood, 2000; Fisher, 2001; Molander et al., 1996). As Fischer notes in the *Journal of Homeland Security* (2001), the "borderless medium of cyberspace [is] a de facto representation of globalization," American extra-territoriality, and therefore, it has become a double-edged sword for the U.S. Since the mid-90s, policy-makers have warned that the Internet "extends the battlefield to incorporate all aspects of society" (Cilluffo, 2000), removing the archetypal boundaries between what is considered domestic and foreign, a crime or an act of war, civilian and military, and local versus global (Anonymous, 1998; de Borchgrave et al., 2000; Fisher, 2001; Molander et al., 1996). As reviewed in Chapter Two, Agnew (1994, 1998, 1999) and O'Tuathail (1998) note that concepts of economic and political sovereignty are increasingly changing and disappearing in the contemporary geopolitical order. The Internet has come to play a prime role in this metageographic shift (Taylor, 2001), disregarding all societal norms based upon territorial affiliation and upon which state security has always been based. There are "no front line[s]" in cyberwar (Fisher, 2001). A crime does not necessitate a full military retaliation, but if someone in Indonesia steals information from a Pentagon computer, the crime does not fall under the jurisdiction of law enforcement either, as it is an international incident (Anonymous, 1998, p. 14-17, 40). Purposefully targeting a telephone network in a major U.S. city might be viewed as an attack against public services and the civilian population, but at the same time, 95% of the Defense Department's communications travel across privately owned networks, making it a perfectly rationale military target (Cilluffo, Collins, Borchgrave, Goure, & Horowitz, 2000; Fisher, 2001). Such blurring of traditional social boundaries in the rules of conflict presents a real challenge to policy makers. For as the Chief of the National Infrastructure Protection Center (NIPC) notes: "There's no way to draw a line around the continental United States and say that our information infrastructure belongs to us" (Anonymous, 1998, p. 4).

Of particular concern and recognition to policy makers and defense experts is that the Internet offers anti-hegemonic elements a prime medium for asymmetrical warfare – the ability to stealthily attack strategic targets with forces much smaller than those of the opposition (Anonymous, 1998; de Borchgrave et al., 2000, p. 8; Larsen & David, 2000; Molander et al., 1996, p. 30). Undefeatable in head-to-head military conflict, the RAND and NSF funded Center for Strategic and International Studies concludes that any "successful challenges [to U.S. hegemony] must be indirect or asymmetrical" (Cilluffo et al., 2000, p. 2). With more of its critical infrastructure and communications based on the Internet than any other state, the U.S. will not only find itself far more susceptible to this type of attack than other states and institutions, but unable to counterattack with nearly as much consequential impact or effectiveness (Cilluffo et al., 2000, p. 2). As William Ware notes in a RAND document analyzing risks and strengths of the U.S. information infrastructure: "Computer systems … are increasingly opening their databases and systems to general public access for enhanced services, and consequently will be exposed to a broader threat spectrum" (Ware, 1997). Compounding the threat is the fact that complete and total security against online attacks is highly unlikely, because of a "deep-seated new peril in the cyber-dimension, where the facility to network has outpaced the ability to ensure security" (Fisher, 2001).

Innovators and developers, the individual hackers that have been behind the evolution of the Internet since its inception, remain one step ahead of government and corporate security measures. In the *Journal of Homeland Security*, David Stephenson argues that the "reason for the [security] gap is the lag between new technology and internalizing new ways of thinking to capitalize on it" (Stephenson, 2002). While the U.S. has the same technology as its adversaries, if not better, it has difficulty adapting its institutions and evolving its processes to utilize this technological advantage. This has led studies to call for "[n]ew organizational structures" and a "restructuring of [the] missions and goals" of agencies at the Federal level (Molander et al., 1996, p. xvi). A RAND report for the Air Force notes that "designing organizational structures that can evolve [during the information age] is so important" but any "premature restructuring of organizations is … risky" (Buchan, 1996, p. 17-18). Until the U.S. does modernize its thinking and organization to better embrace the information networks behind its position of power, online, asymmetrical warfare will offer an equal playing field to non-state actors, individuals, and nation-states alike, to begin contesting United States hegemonic leadership (Anonymous, 1998; de Borchgrave et al., 2000).

For sometime now, U.S. policy-makers have begun echoing the warnings of academics that “[t]he onset of the information age has decreased the power of states and other mass hierarchal organizations” (Cilluffo et al., 2000, p. 3) and provided new agencies increased opportunities to “weaponize” and threaten “United States soil” (de Borchgrave et al., 2000, p. 3). Yet, though recognition is given to the fact that “[d]isrupting national objectives does not require as much time or as many actors as it once did” (de Borchgrave et al., 2000, p. 11), that non-state actors are increasingly becoming “important subsidiary actors in international relations” (Cilluffo et al., 2000, p. 3), and that “[n]ew actors must become part of the national security equation” (Cilluffo et al., 2000, p. 1), the U.S. government and its defense forces have been particularly loath to fund studies concentrating on such threats, instead emphasizing the threat of information war from other territorial states (de Borchgrave et al., 2000, p. 8; Molander et al., 1996).

Of particular concern to the Department of Defense has been a potential “information war gap” with traditional geopolitical adversaries. Several military journal pieces published in China have illustrated the People’s Liberation Army’s (PLA) focus on developing information warfare techniques and weapons in order to facilitate inter-state conflict (Fisher, 2001; Gill, 1996; Mulvenon, 1999). The United States and Russia have both been developing “cyber-war machines” as well (Messmer, 2000), but of worry to the Department of Defense is the fact that defense mechanisms against inter-statal cyber attack remain elusive (Molander et al., 1996). Of particular concern to national security personnel is the threat of an adversary swarming – launching an asymmetrical, multi-faceted attack against – the networks that the U.S. military relies upon (de Borchgrave et al., 2000, p. 11). Though a conventional attack on the U.S. military, such as the bombing of the U.S.S. Cole, offers a blow to feelings of security, it actually does little to directly threaten the U.S. (de Borchgrave et al., 2000, p. 11); whereas a coordinated cyber-attack on the U.S. military could threaten the very infrastructures upon which U.S. security functions (Anonymous, 1998; Arquilla & Ronfeldt, 1999b, p. 59-61; de Borchgrave et al., 2000, p. 11; Fisher, 2001; Molander et al., 1996; Ware, 1997).

Of potentially more danger to national security is that the information age "has empowered individuals and non-state actors" (Cilluffo et al., 2000, p. 1) around the globe that may "perceive justifiable reason to challenge America's leadership" (Larsen & David, 2000), particularly during U.S. hegemonic decline. If facing state actors in cyber conflict, the U.S. maintains the resources and diplomatic strength to defend itself and conduct counterattacks. However, as the RAND funded Center for Strategic and International Studies noted in its report on Defending America in the twenty-first century, "[t]he onset of the information age has decreased the power of states and other mass hierarchical organizations" (Cilluffo et al., 2000, p. 3) against non-state actors. The U.S. finds itself in the undesirable position of facing incalculable risks, requiring rapid modernization to counter the rise of new types of adversaries. The problems associated with defining the agencies behind online attacks against the U.S. are multifaceted: an attack often remains unnoticed, at least initially, due to poor surveillance of computer systems, and once an attack has been identified, it may remain difficult to establish the place of its origin or when it was implemented, much less who is actually responsible for it, so that a retributive attack might occur (de Borchgrave et al., 2000, p. 44; Larsen & David, 2000).

The threat of information warfare has procured numerous antidotal policy suggestions and recommendations from RAND and ANSER affiliated parties and experts (Anonymous, 1997; Buchan, 1996; Cilluffo, 2000; Ware, 1997). Though many studies spend much of their agenda concentrating on strategies for combating cyber-warfare between nation-states (Anonymous, 1998; Buchan, 1996; Cilluffo et al., 2000; Cilluffo, 2000; Dorobek, 2001; Fisher, 2001; Molander et al., 1996; Mulvenon, 1999), much policy has also attempted to emphasize defense against asymmetrical attacks from non-state agents (Anonymous, 1998; 2001; Arquilla & Ronfeldt, 1999a, 1999c, 2001a, 2001b, 2001c; Cilluffo et al., 2000; Cilluffo, 2000; de Borchgrave et al., 2000; Fisher, 2001; Ronfeldt et al., 1998). However, one thing in common links all policy documents, an urgent and inherent call for drastic modernization of state defenses against network weaknesses.

## A Hegemonic Headache: U.S. Attempts at Reflexive Modernization

As discussed in the previous chapter, reflexive modernization is an inherent and ongoing aspect in contemporary "risk society" (Beck, 1992). Beck (1992) defines reflexive modernization as occurring when institutions with political power have allowed inherent and overwhelming risks to procure and proliferate under their jurisdiction in order to gain from the benefits of these risks (e.g., nuclear weapons and power, environmental degradation, et cetera). The institutions established before these risks come to fruition (e.g., the state, or sub-state institutions, such as the Department of Defense) must continually and reflexively modernize to the dynamic evolution of side effects stemming from the technological development from which they benefit and continue to proliferate (e.g., the Internet). Primarily concerned with nuclear weapons and the influence they had on the rise of sub-politics, Beck (1992) emphasized that if established institutions of power failed to reflexively modernize to handle the societal risks they had created, sub-politics would rise in an attempt to discard the outdated institutions of power and create new ones capable of handling the risks.

In the end, for the most part, the inter-state system has been able to reflexively modernize and diffuse the risk of global nuclear holocaust to a limited extent, but today the Internet presents a new, and perhaps more threatening, risk. For as Fisher notes in ANSER's online *Journal of Homeland Security*, "protection of core values or vital interests within a sovereign space is one of the more universally accepted premises of [national] security" but today "the applications and processes [the Internet and networked telecommunications] have engendered, do not succumb to territorial and geographical restraints" (Fisher, 2001). He goes on to state that "[w]hereas nuclear weapons may be more potent in destructive capability, cyberspace 'unbundles territory' more completely" (Fisher, 2001). Thus, a primary need for the United States and Federal agencies, as well as all political institutions based on territory worldwide, is to reflexively modernize to the inherent plethora of risks stemming from the Internet. How to best go about any such modernization, however, lies at the center of much debate coming out of RAND and ANSER policy camps (Anderson, 1999; Anonymous, 1998; Cilluffo et al., 2000; de

Borchgrave et al., 2000; Dorobek, 2001; Frank, 2001a; Garamone, 2001; Lemos, 2001; Stephenson, 2002; Vaida, 2001; Ware, 1997).

The evidence that the U.S. government is attempting to reflexively modernize, without explicitly realizing it, is evident in the predominate strategies that continue to resurface from ANSER, RAND, and other affiliated organizations, concerning defense against information warfare. Though "recommendation" and "implementation" are rarely synonymous in the political world, after the terrorist events of September 2001, the Bush Administration established an official Office of Cyberspace Security (Anonymous, 2002g), and in the handful of months since, many policies recommended by RAND and ANSER have finally sprung from rhetorical discussion to the preliminary stages of incursion. Policy and modernization recommendations have included: creating an early-warning system similar to the one meant to alert institutions of nuclear attack during the Cold War (Cilluffo, 2000; Lemos, 2001; Vaida, 2001; Ware, 1997); forming a central command center for defending against information war (Garamone, 2001; Vaida, 2001); establishing a separate Net for the Federal Government, GovNet (Frank, 2001a, 2001b; Lemos, 2001); legislating corporate liability for security glitches in software (Anderson, 1999; Anonymous, 2001); and forming a partnership with the private sector, primarily large corporations, to share in the responsibility, and more importantly the costs, of cyber-security (Anderson, 1999; Anonymous, 1997, 1998, 2001; Cilluffo et al., 2000; Cilluffo, 2000).

A desire to establish an early-warning system and central command center is of little surprise when one remembers the nuclear-winter frame of mind from which many of the Pentagon and policy makers come. It is argued that if a regular level of information network interference – "background noise" – can be established, then vigilant monitoring of the Internet will tip U.S. defenses off to a massive or coordinated attack against critical infrastructures, i.e., power grids, telecommunications networks, FAA control towers, the financial system, et cetera (Cilluffo, 2000). As Ware notes in his RAND study on cyber defense, "[w]e need to establish what the engineering community would call the 'noise level' in the infrastructure" as a particular background "noise characterizes the normal state of affairs, some aspects of which are statistically predictable" (Ware, 1997). Ware goes on to state that putting an early warning system "in place together with a coordinating center [would] provide a dynamic overview of unusual or abnormal activity" on the Internet (Ware, 1997). In the *Journal of Homeland Security* too, Larsen and David argue that "[a]n integrated warning/information … system is required to ensure effective use of resources to mitigate effects during and after large-scale attacks and campaigns" (Larsen & David, 2000). Theoretically, an early-warning system would solve the problem of "when" and "how" a cyber attack is coming. Yet, even studies looking into this theoretical system are primarily done under the assumption that U.S. interests will be attacked by another state in conjunction with conventional forces (Mulvenon, 1999; Vaida, 2001).

The idea is that an early-warning system would be used in similar vein to the nuclear warning system of yesteryear – identifying large-scale, all out attacks on the U.S. This is demonstrated in the CSIS's call for the invention of "INFOCON," to be used in tandem with the Department of Defense's DEFCON system (Anderson, 1999, p. 58). The effectiveness such a system would have at identifying localized swarming – that is asymmetrical warfare against one particular node – or of preventing individual attacks is likely minimal, as small or medium scale attacks would be difficult to recognize from the standard noise of the Net. Moreover, the argument for the creation of an early warning system is based on defending against attacks on the U.S. homeland, but studies have thus far failed to clearly define how this system would defend U.S. interests and institutions globally (e.g., embassies and U.S.-based corporation networks not within the United States).

The construction of a new, secure government network within Federal agencies that evades inter-connectivity with the Internet may also offer a solution to thwarting hack attempts from online users (Frank, 2001a; Lemos, 2001). Though rarely discussed in policy itself, U.S. head of Cyber-security, Richard Clarke, continually endorses the formation of a separate government information network, aptly referred to as GovNet (Frank, 2001a, 2001b; Lemos, 2001; McCullagh, 2002). Unfortunately, the ability to keep GovNet separate and disconnected would not only require a new computer protocol but the construction of an entirely new communications infrastructure (Frank, 2001b). For GovNet to truly work independent of the Internet's network infrastructure, new satellite systems and fiber optic infrastructures would have to be built (Frank, 2001b). Furthermore, the threat of an inside attack, coming from anyone with access to GovNet, remains just as conceivable as that of a hacker using the current telecommunications network to break into such a network (Ware, 1997). Though GovNet has the backing of the National Security Council, it has not been entirely embraced by actual policy makers, and some in the private sector have deduced that "[a] massive, completely partitioned government network is a pipe dream" (Frank, 2001b, citing Forrester Research, Inc.).

Perhaps a more realistic, and more important, approach at security than the restructuring of the government's communications infrastructure is found in the unanimity of RAND and ANSER publications calling for security cooperation between the private sector and government agencies (Anderson, 1999; Anonymous, 1998; Arquilla & Ronfeldt, 1999b; Cilluffo et al., 2000; Cilluffo, 2000; de Borchgrave et al., 2000; Stephenson, 2002; Ware, 1997). This is viewed as such a crucial step in establishing U.S. security, that it has included policy calls for reneging or modifying the Freedom of Information Act to help induce corporations to begin sharing information about security breaches and financial losses accrued via cyberspace (Anonymous, 1998; Cilluffo, 2000). As Stephenson notes in the *Journal of Homeland Security*, "with most American communications infrastructure owned by the private sector, partnership is a necessity" (Stephenson, 2002). He believes corporations must realize that their security depends on helping the U.S. identify cyber-security breaches (Stephenson, 2002). Other policy makers concur, stating in White Papers to President Bush and journal articles alike that "[c]ooperation … is the only effective way to combat" the problem of Internet security (Anonymous, 2001, p. 6), and "Silicon Valley and the Beltway … must stand side by side and on equal footing in addressing [cyber] issues and formulating responses" (Cilluffo, 2000). Fisher (2001) espouses that the private sector and international telecommunications companies will become “key player[s]” in the effort to secure information in cyberspace.

One of the main impediments to corporate partnership with the government, though, is that any information provided to the government about attacks or electronic break-ins is open to public scrutiny through the Freedom of Information Act. As the Head of ANSER notes, “[t]oday, corporations, large and small, are less than enthusiastic partners” due to three reasons: 1) reporting cyber crimes to the government can lead to a disruption in business; 2) allowing one’s computer networks to be investigated by the state may provide self-incriminating evidence about business practices; and 3) most importantly, allowing the government to come, or reporting the details of a cyber crime, may compromise highly sensitive propriety information (Larsen & David, 2000). Corporations are rightfully loath to inform the government about network breaches, as doing so will result not only in bad publicity but, pending the enormity of the cyber break-in, plummeting stock prices. Due to corporate unease about sharing information with the government, it is estimated that less than 10% of all cyber attacks are reported (Cilluffo et al., 2000, p. 5).

Policy papers are quick to note that the private sector’s unwillingness to cooperate with the government is not based solely on the Freedom of Information Act, but also stems from the government’s folkloric ineptitude in helping corporations with online security to begin with (Cilluffo et al., 2000, p. 23; de Borchgrave et al., 2000, p. iii). As Ware explicates in his document reviewing the state of cyber security, “[v]arious study groups, advisory boards, etc., have addressed the issue [of leading by example] and flagged its importance to the government, but the prevailing opinion continues to be that *federal computer-systems and network security is not in an adequately strong posture*” (Ware, 1997, emphasis in the original). Realizing this problem a new institution, the National Infrastructure Protection Center (NIPC), was established in 1998 within the Department of Justice to begin a dialogue between the Federal government and private sector. The NIPC was originally schemed to be a center through which private and public security information might be accumulated and shared, but thus far it has remained a largely dormant institution. Partnership with this new government institution quickly came to represent a unidirectional flow of security information – from the private sector to the government, not vice-versa (Cilluffo et al., 2000; de Borchgrave et al., 2000).

Still muddled in conflicting ideologies, those fermenting from the Cold War era and new ones sprouting from the information revolution, in recent years U.S. policy has offered various antipodal remedies for homeland defense from cyberspace. This may be the most vexing problem facing U.S. cyber policy – the inundation of antithetical ideas concerning reflexive modernization for network security emanating from a state-focused military-industrial complex. Information warfare strategy is heavily influenced by military and non-profit organizations steeped in classic geopolitical and national security thinking – e.g., the Department of Defense, RAND, ANSER, and other such entities. This in turn often leads to defense and security methodologies relying on territorial and hierarchal organizations from the Cold War geopolitical order (Brzezinski, 1998; Gray, 1988, 1999). At first sight this logic makes sense, as the U.S. military and government are inherently constructed and organized within a territorial demarcation. However, as RAND analysts Arquilla and Ronfeldt note to no end, one of the most dangerous things about any information war policy is that it is based on false assumptions that do not pertain to networked conflict (Arquilla & Ronfeldt, 1999b, 1999c, 2001a, 2001b). The only way to beat an adversary using network organization and asymmetric warfare is through network organization and asymmetric means (Arquilla & Ronfeldt, 1996, 1999c, 2001a, 2001b, 2001c).

## Spatial Dementia: U.S. Policy and the Realities of Network Conflict

> "*Terrorist and outlaw states* are extending the world's fields of battle, from physical space to cyberspace…" – Bill Clinton (Fisher, 2001, emphasis added)

Out of all the government funded risk assessment projects (Anderson, 1999; Anonymous, 2001; Arquilla & Ronfeldt, 1996, 1999b; Cilluffo et al., 2000; de Borchgrave et al., 2000; Mulvenon, 1999; Ronfeldt et al., 1998), the white papers presented to the President and

Congress (Anonymous, 2001), and the experts writing on Net War (Anonymous, 1997; Buchan, 1996; Dorobek, 2001; Gray, 1999; Molander et al., 1996; Mulvenon, 1999), one overriding element remains clear – a vast majority are underscored with traditional territorial, state-versus-state, strategic prognosis. Some policy makers outright deny any need to change overall conflict strategy due to the advent of net war (Gray, 1999, p. 248-250, 267-270); however, most experts concur that "[a]ttacks leveled in cyberspace defy all forms of physical impediments" and foster an "ambiguity … at almost every level" of defense (Fisher, 2001). Yet, the recommendations and strategies that these same experts provide to counter the cyber-threat are often tainted with territorial assumptions and hierarchical organization procedures that only further induce a type of spatial dementia in U.S. policy and defense preparation.

The territorial hang up overshadowing policy making becomes evident in the recent change of semantics concerning state security – from "national security" to "homeland defense." Discussing U.S. security in the *Journal of Homeland Security*, ANSER's Executive Director, Ruth David, and coauthor Randall Larsen, proclaim:

> "In the 21st Century, the term 'homeland defense' is nearly synonymous with how we used the term 'national security' in the latter half of the 20th Century" with two differences: "some non-state actors have the capability to bring a new form of warfare to the American homeland … [and] new types of weapons are immune to our superpower status and traditional defenses" (2000).

Such discrepancies between terminology and reality – if there is one major difference about national security today as opposed to during the Cold War, it is that there is no explicit "homeland" left to defend – are typical side-effects of the U.S. attempting to reflexively modernize to a deterritorialized geopolitical order. Policy, such as that produced by ANSER and RAND, has begun to note the changing realities of national defense, but at the same time is becoming even more territorially fixated.

The deterritorialization of power in world politics is responsible for the confusion plaguing the U.S. over "homeland defense" right now. State security has always been linked to territory, and attempts to maintain security without territoriality "make[s] for a conceptual morass" (Fisher, 2001). Though doubtlessly the "Federal government will [continue] to play the leading role in deterrence, prevention, preemption, attribution and retaliation" in homeland defense as it always has (Larsen & David, 2000), it will be forced to modernize or be subsumed by sub-politics in a deterritorialized landscape. This has been recognized at RAND and ANSER, and even emphasized in the *Journal of Homeland Security*: "Homeland defense is a new concept for America, requiring new ideas, new partnerships, and vigorous debate" (Larsen & David, 2000).

However, new forms of thinking aside, it is the failure to recognize that an inalterable, metageographic shift is what lies behind the new risks that are forcing modernization that will continue to hamper the world hegemony's ability to cope with online threats. As confusion continues to reign in policy debates, the lawmaking process is often misguided into inadvertently making new reallocations of defense resources even more difficult. Cilluffo (2000) laments that "without leadership the entire [security] structure crumbles, because policy priorities are sustained only if they are supported by political will and the necessary resources." Lacking strong leadership and political will, policy fails to become streamlined, often resulting in counterproductive actions. As was noted at the Seminar on Cyber-Terrorism and Information Warfare in 1998:

> "The convergence of [network] technologies made some laws, made some procedures, made some understandings obsolete. And very, very well meaning people in the policy area now … are rushing to produce laws and procedures to protect us from cyber-terrorism, from piracy, from economic attacks. At the same time, they are jeopardizing our own ability to deal with those subjects" (Anonymous, 1998, p. 9, quote of Dr. Frieder).

Perhaps nowhere do such outmoded laws, procedures, and understandings, come to light as much as in discrepancies between the Department of Justice and the Department of Defense. As the Pentagon suffers an increasing number of electronic intrusions every year – many of which go unnoticed – the absurd truth is that it remains primarily preoccupied with preparing for information war in inter-state conflict. And though the FBI is in charge of protecting U.S. critical infrastructure, most of which is connected to the Internet and therefore susceptible to cyber attack, it finds itself with little or no jurisdiction to pursue attackers when it determines that an attack comes from overseas – for that is a military matter (Anonymous, 1998, p. 3-8). The binary between *domestic* and *international* (Agnew, 1994, 1998) defense contaminates the designation and creation of separate cyber-security tasks to government institutions as such decisions on delegation are often based on agencies' historical role in national security. Yet, not only does cyberspace fail to breakdown into domestic and foreign spheres, a majority of adversarial agents operating on the Net are rarely connected to any territorially based organizations upon which U.S. agencies' jurisdiction and authority to retaliate depends and functions.

For example, if a Swiss individual affiliated with an environmental organization (e.g., the Green Earth Movement) were to shutdown a coal plant in Ohio through the Internet, the options available to the U.S. would be limited under international law. Affiliation with the Green Earth Movement does not imply that the organization endorses such action, and as the organization is international in scope, U.S. sanctions against the non-state actor would be of minor consequence and little deterrence. Moreover, Switzerland as a state institution is certainly not responsible for the attack on U.S. infrastructure; thus, military retaliation on Swiss infrastructure is not warranted or permissible under international law. Such real life scenarios led one RAND report to conclude that "key national military strategy assumptions are obsolescent and inadequate for confronting the threat of I[nformation] W[ar]" (Molander et al., 1996, p. xvii). Yet, the same report refers to the "vulnerability of U.S. homeland" to strategic information warfare, displaying a continued and inherent territorial bias.

Wise to the limitations of current institutional jurisdictional structuring, numerous policy makers and defense experts at RAND and ANSER have begun to focus on prevention of cyber-crime over enforcement and reactionary measures. At the Seminar on Cyber-Terrorism and Information-Warfare (1998), the need to stop trying to prosecute individuals after an attack and instead begin instituting policies that make attacks more difficult was repeatedly espoused. As Cilluffo (2000) notes, "[T]oo much emphasis has been placed on catching the perpetrators after the crime, rather than keeping them out in the first place" and as the Center for Strategic and International Studies report notes: "[D]efense efforts have been reactive, disjointed, and focused on post facto consequence management" (Cilluffo et al., 2000). Organizational issues such as the NIPC falling under the Department of Justice's jurisdiction have been increasingly criticized, as the Department of Justice is not historically aligned toward prevention but prosecution (Cilluffo et al., 2000). In order to counteract this unfortunate juxtaposition between Federal institutions roles in homeland defense and the reality of cyber security, policy makers have little choice but to look toward partnering with other states and the private sector to defray the enormity of this security task. It has been argued that one carrot to gain the support for cooperation from trans-national corporations – which as discussed earlier in this chapter, has been hampered by the U.S. government agencies' own ineptitude – might be found in the legal establishment of a protocol for information assurance (Anonymous, 1998, p. 24-26; 2001; Cilluffo, 2000; Frank, 2001a).

Information assurance has become a central facet of reports concerned with homeland defense. Information assurance is defined as "the information operations that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and nonreproduction" (Anonymous, 2001, p. 2). Proponents of the need for prevention over enforcement argue that only through informed legislation accounting for a certain amount of corporate liability in protecting their networked systems can paramount changes be made to national security (Anonymous, 1998, p. 14-17; Frank, 2001a). Essentially blaming software developers for not taking enough responsibility for glitches and backdoors in their programs and security software (Lemos, 2001), some policy makers would like to tighten Internet security through the enforcement of minimum guidelines on all new software and computer products (Anonymous, 1998; Frank, 2001a). This policy argument is akin to that of holding a manufacturer liable if it places a car on the market that has not been tested for dangerous quirks. As entirely glitch free software and networks will never be possible, more promising still for securing online networks is the establishment of laws that limit the liability of corporations running a designated standard of security (Cilluffo et al., 2000, p.

24). At first such policies appear to offer better methods of securing the private networks upon which U.S. security depends, by bringing the private sector to a standard level of security, but under closer scrutiny, they are still based on a false sense of territoriality that is increasingly nonexistent.

Though there is little doubt that standard security measures across the board would benefit the United States government's ability to secure cyberspace, seeing as "critical infrastructures are owned and operated by the private sector for the most part" (Anonymous, 1998, p. 8), it would be foolish to disregard the complexity of enforcing such U.S. backed standards globally – particularly during this time of hegemonic decline. As transnational corporations and telecommunications infrastructures span the globe, it is difficult to justify why U.S. standards and laws would apply globally, much less under what pretext. Furthermore, being at the end of its hegemonic cycle, the U.S. is unlikely to garner the kind of support needed to reach international consensus on such laws. As Fisher (2001) recently noted in an online ANSER publication, online businesses "and the applications and processes they have engendered, do not succumb to territorial and geographical restraints." Once again, legislation on information assurance may be well meaning, but in fact might actually further complicate the modernization of institutions to deal with online threats (Anonymous, 1998).

Due to the complexity of garnering support behind any particular information assurance policy, RAND and ANSER publications seem to concur that an avenue of equal cooperation, indeed, power sharing, between the U.S. government and corporate sector holds the greatest chance of success for buffering U.S. homeland defense against online incursion. As the ANSER affiliated Center for Strategic Initiative Studies (CSIS) notes in their report on cyberthreats and homeland defense, "[state s]ecurity is now the responsibility of each company, government entity and private institution" (de Borchgrave et al., 2000, p. iii). It is argued that through cooperation with private industry, and between Federal agencies themselves, the U.S. might nip security holes in the bud and forge a process of information sharing that would thwart potential online attacks in the early stages (Anonymous, 1998; Cilluffo, 2000; Molander et al., 1996, p.

xviii). Though not articulated in policy, this argument is based on the fact that trans-national corporations, already globally networked, are likely far more capable than any territorially based entity, including the U.S. hegemony, at providing security at the international scale. The former Director of the NIPC, Michael Vatis, views information sharing and trust between the corporate sector and government agencies as the fundamental ingredient to successful information network security (Anonymous, 1998). He goes on to argue that the U.S. is incapable of securing itself from online attacks alone and that:

> "[P]rivately owned infrastructure operators have a big role to play in this. [Security] is not something law enforcement can do alone. It's not something the Federal government can do alone" (Anonymous, 1998, p. 8).

During every hegemony's decline, power sharing and cooperation with other powers has occurred to ensure the seas stay open for trade (Arrighi, 1994; Arrighi & Sliver, 1999). Traditionally, these other powers were semiperipheral or core states that were considered regional powers and had an interest in helping the hegemony maintain the capitalist world-economy. The Dutch aligned with the British in such a fashion, Britain garnered the support of the U.S., and today, it appears, a similar happenstance might be forthcoming with the U.S. aligning with trans-national corporations. Though the medium of capital exchange has changed – from shipping goods on the open seas to packeting information across the fiber optic virtual world – it is of crucial importance to the hegemony that the Internet become secure, so that maximum profitability can be gained from networked commerce.

Arrighi and Silver argue that one of the driving impetuses behind declining hegemonies making such alliances with regional powers is cost. Enforcing secure and open trade on a global scale becomes too expensive and burdensome for a hegemony in economic and political decline, and delegating capitalist world-system maintenance chores through alliances proves far more efficient (Arrighi & Sliver, 1999). Today, as the U.S. calls upon corporations to help secure online commerce, finance, and trade, certain parallels between the U.S. and British hegemonies become evident.

Of course, rhetoric about full cooperation aside, the U.S. would not view a partnership with the private sector as being truly equal. Certainly any cooperation between the private sector and the hegemony would not be so either; though, like a bad marriage, the partnership may soon thereafter mutate into something that the suitor had not originally foreseen. The carrot on the stick that might lure the corporate sector into such a partnership is the promise of tougher laws on information disruption and perhaps, with the help of U.S. extraterritoriality, more global cohesiveness between states in pursuing criminals responsible for attacks. As Cilluffo notes, "[O]nly through leading by example, by getting its own house in order, can the government realistically hope for the private sector to commit the sort of resources expected of it" (2000). The U.S. will find itself in a dire position if it cannot persuade the private sector that partnered enforcement of online security is beneficial to all, as any "state that places its critical infrastructures under the control of information technologies can no longer rely on geographical boundaries or benevolent neighbors to buffer these systems" (Fisher, 2001). Perhaps recognizing deterritorialization's role in the current security predicament more than any other ANSER or RAND analyst, Fisher predicts that "[d]ue to the lack of borders and boundaries in cyberspace it has become impossible to strictly demarcate and secure [the Internet]," and therefore, "the private sector will become key players in any nation's efforts to secure their information systems from foreign governments, terrorists, and lone hackers" (Fisher, 2001).

Though likely appearing benign, any eventual partnership between the U.S. and the private sector would be a clear sign of, indeed facilitating process behind, hegemonic decline. It would symbolize the hegemony acquiescing its dominant role as sole defender of hegemonic interests in the world-economy – ceaseless accumulation of capital through expansion of the world-system. The U.S. would thereby be admitting that the Department of Defense, FBI, and other government agencies are incapable of safeguarding the "homeland" from Internet invasions on their own, instead reflexively modernizing by diluting their powers and sharing with non-U.S. actors. Unfortunately for continued U.S. hegemony, with the deterritorialization of politics, there may be few alternatives other than to establish such partnerships.

With a vast majority of communications infrastructure lying in the private sector, and the expenses involved in monitoring and regulating the Internet impossible to imagine, the U.S. needs the private sector to have any hope of quelling the growing wave of online attacks. With adversaries from everywhere in the world utilizing the U.S. information infrastructure's "hundreds of thousands of entry or access points" (Anderson, 1999, p. 1), the futility of territorially aligned strategies and political processes is summarized succinctly by Lt. Colonel Walter Sharp: "Not only does this technology bring conflicts to our soil without troops having to land here, but this technology will bring conflicts to our soil and will make more civilians and civilian infrastructure a lawful target under the laws of our own conflict" (Anonymous, 1998, p. 17). Only through corporate diligence and private policing of networks around the globe can attacks truly begin to be stymied.

Like the British and Dutch before, a prime reason for the necessity of this pact between transnational corporations and the world hegemony is that during this period of hegemonic decline, the U.S. is fiscally incapable of continuing to ensure secure global trade on its own. The modernization of U.S. agencies and institutions to a deterritorialized world order is not an inexpensive process. As has been shown by U.S. attempts to change agency roles in the wake of the September 11th attacks, not only do political debates surround what modernizations should take place (e.g., Federal employees in airport security) but also how much money should be allocated to such changes. Part of any forthcoming alliance with the corporate sector would be an effort by the U.S. to stymie the costs of global leadership and defense against potential, and as of yet primarily unseen, online enemies. Of course, no matter what should happen, the U.S. will remain an active part of the defense process, both fiscally and politically, but its main role may be reserved to funding research and development of network security, followed by promoting and overseeing such security developments' implementations in the private sector (Anonymous, 2001, p. 5; Cilluffo et al., 2000, p. 24). Such a fiscal role for the U.S. has already begun, as was illustrated by the recent passing of a House bill providing $800 million in NSF grants to universities for preliminary research on enhancing computer security and the establishment of network security curriculums (Hopper, 2002).

As Homeland Defense Secretary Tom Ridge recently noted, “There is a status quo in Washington. People comfortable with doing things the twentieth century way aren’t willing to start doing things the twenty-first century way” (2002e, paraphrased). Herein lies the decisive problem facing the U.S. in cyber-security: the new spatiality behind network conflict must be recognized and understood before any reflexive modernization of Federal agencies’ organization and roles can effectively take place. As U.S. policy and defense strategy is still heavily influenced and prejudiced toward a territorial spatiality that does not exist online, reflexive modernization of homeland defense will remain ineffective and direly incompetent against the rising wake of hegemonic adversaries using the medium of cyberspace. In failing to properly recognize that online threats stem from a new form of geographic organization – the network metageography – the U.S. futilely exerts its energies by attempting to prevent traditional enemies (e.g., territorial states such as China) and a plethora of anti-systemic movements (non-state actors) from attacking the U.S. via cyberspace. In reality, many sub-politics utilizing the Internet are forming due to the lack of political stability during the current period of hegemonic decline, as well as, the United States’ utter failure to reflexively modernize to the contemporary risks that the network geography of the virtual world brings.

As can be witnessed by the plethora of contradictory and vying policy recommendations coming from ANSER and RAND sources, it is far more difficult for the U.S. to gain the levels of consensus needed to modernize to the network metageography than it is for new sub-politics to form. This is glaringly obvious when the sub-politics forming are already inherently decentralized, non-hierarchically based, and interconnected at the global scale via the telecommunications network. While U.S. policy has been struggling to reflexively – though perhaps more accurately in this case, reactively – modernize its government institutions “toward an American information strategy” (Arquilla & Ronfeldt, 1999b), sub-politics have been finding success online for years and are, as concerns continued U.S. hegemony, dangerously ahead of the curve (Arquilla & Ronfeldt, 1999c, 2001c). As Arquilla and Ronfeldt (1996, 1999a, 1999b, 1999c, 2001a, 2001b, 2001c) note, those who organize and use networks first have an unprecedented advantage over those who only later begin to adapt from a territorial outlook to one of interconnectivity. Though the U.S. holds technological and economic superiority over its potential adversaries, the longer it takes to develop network capabilities and strategies, the greater an uphill battle it will face (Arquilla & Ronfeldt, 1996, 1999c, 2001b).

As will be illustrated in the following chapter, today sub-politics have begun to garner incredible strength due to their effective use of networking capabilities found on the Internet. Organizations that in the past were confined to national or regional organization are now able to organize in nodal matrixes, with territorial affiliation of their agents representing nothing more than a node in a network of activism. As the U.S. continues to struggle modernizing to the new network metageography, new political institutions centered around contemporary issues and risks concerning global society – environmental issues, human rights abuses, economic disparity, gender equality, freedom of information, et cetera – have proliferated. Seen as real potential adversaries in contemporary U.S. policy, the U.S. will likely need to adapt its institutions to counter such movements, as well as stymie the risks around which they form, or face an increasing onslaught of cyber-conflict.

## Conclusion

U.S. cyber-security is wrought with contradictions: territorial organization in the face of network conflict; political institutions based on waning geopolitical orders; lack of intra-agency consensus on how best to tackle information warfare, prevention versus enforcement; critical components of U.S. security relying almost entirely on privately controlled networks; and no real method for deterrence or prevention of information warfare, just methods of reactive management for when it does occur. The U.S. government is attempting to modernize its position and abilities in homeland defense against network warfare, but due its own territoriality and hierarchal power structure, it is ignorant to the inherent need for change in spatial perspective and organization behind any such successful defense strategy. Thus, a window of opportunity has arisen for sub-politics and anti-systemic movements to proactively use the medium of cyberspace to confront the U.S. and the political institutions behind its hegemonic position (e.g., the U.N., WTO, the Department of Defense, and critical infrastructures). As will be shown in the following chapter, new sub-politics and old anti-systemic movements abound in cyberspace, and they hold a drastically variant perspective from the U.S. concerning the political geography of online agency.

As sub-politics and anti-systemic movements organize against particular risks and around various doctrines – many of these risks and issues being associated with the prime modernity of the world hegemon – the U.S. is placed in a precarious position. For while it accumulates more economic, political, and social advantage from the global reaches of network telecommunications, it will increasingly find itself the target of sub-politics. Its political borders inconsequential, its communication networks perpetually fallible, and standing as the poster child of all gluttony associated with ceaseless capital accumulation, the U.S. will increasingly represent a ripe target. Until it begins to modernize its role and its institutions around the reality of a deterritorialized political landscape, the U.S. will continue to find its interests and homeland threatened. As Fisher well summarizes changes in the future of U.S. defense: "[T]he topography of the world's security landscape will involve actual landscapes less and less" (Fisher, 2001).

Though cooperation with the corporate sector offers one solution in deferring the costs and burden of electronic defense against unseen enemies, it also suggests that the U.S. may be further in the throes of hegemonic decline than appearances indicate. Unable to afford the incredible costs behind ensuring cyber defense of all network systems, and entirely incapable of redoing the Internet from scratch with security in mind, private ownership of a majority of telecommunications infrastructure around the world, in computer manufacturing, and in software development, leaves the U.S. little choice but to align itself with transnational corporations.  The implications of this go above and beyond this thesis, but suffice to say, as will be shown in the next chapter, such an alliance is certain to raise the ire of numerous online movements.

# Chapter Five: Online Agencies as the Pioneers of a Deterritorialized Geopolitics

As the U.S. struggles to reflexively modernize to the Internet and the security issues that deterritorialized geopolitics raise, movements and political agents utilizing cyberspace in various capacities have begun to proliferate and grow in strength. From individual hackers to real world movements using the medium of the Internet to facilitate their causes, the network geography of the virtual world continues to grow in similar fashion to the Wild West of yesteryear – lawlessly and without overarching authority (Loader, 1997, p.4). As this happens, movements concerned with various political issues – from good customer service to environmentalism – have begun to inform, connect, organize, and mobilize individuals around issue identities in a deterritorialized landscape that holds no borders (Brunn, 1994; Luke, 1998; Rheingold, 1995, 2000; Warf & Grimes, 1997).

In cyberspace, deterritorialized political agency intersects with the territorial politics of the real world. However, in opposite fashion to the difficulties faced by territorial institutions in adapting to this new realm of politics, often in conjunction with real world, territorial vitality, non-state agencies enjoy the advantage of fluid movement, communication, and network structuring – they are mobile and diffuse. As will be shown in this chapter, networked political agencies are confident, realize the advantages of cyberspace, and instead of needing to adapt to the new geography of the network, continually help reinvent and shape this space through their actions – constantly developing new methods of access and connections within the virtual network. As Arquilla and Ronfeldt (1999a, 1999b, 1999c, 2001a, 2001b, 2001c) have aptly argued, those that embrace the network geography of cyberspace first hold a distinct advantage over those adapting to it later. And thus, it comes as little surprise that right now, in cyberspace non-state actors have an upper hand over the U.S. hegemony.

This chapter will analyze online subjects' spatial perspectives of virtual conflict, organizational methods, and political capacity on the Net, as well as how these subjects interact with the politics of the territorial world – primarily those of the U.S. hegemonic power. By looking at four organizations – renamed the Socialist Front, Non-Profit Network, Green Earth Movement, and the Feminist Confederacy – and six individuals, who were also given pseudonyms, this chapter sheds light on the deterritorialized structure of, and the network processes underlying, online politics. The cases analyzed here represent both sub-politics and anti-systemic movements, with the individual hackers, Non-Profit Net, Green Earth Movement, and the Feminist Confederacy mobilizing around particular issues and risks, and the Socialist Front representing one of the most steadfast anti-systemic movements in the world-system. All of these agencies utilize the medium of cyberspace differently but for the same reason – its ability to act as an appendage for broadening the scope of their agenda. Moreover, this chapter will conclude by shedding light on the potential implications the geography of these politics will have on United States power.

What follows is a discussion briefly reviewing the historical role of individual agency, primarily that of hackers, in virtual space. After this, analysis of the hacker data will commence. Analysis will be broken down into: a) how the subjects organize themselves online, and how they use the network of cyberspace to facilitate their goals and aspirations (e.g., methods of communication, organization, and use); b) the perceived spatiality and scale of their actions; and c) their perspective on issues of regulation and conflict with organized political powers (e.g., the U.S.). Following analysis of the hacker interviews, the same will be repeated for hacktivist and online movements, though in a slightly variant order. The chapter will conclude by tying all of the above analysis together into a succinct observation – non-state actors hold a profound edge and advantage in a deterritorialized geopolitical landscape.

## Rogue Agencies: Hackers and Their Place in Cyberspace

Arguably, hacking is more fundamental to the Internet's existence than any other human agency operating therein. As discussed in Chapter Three, today's Internet was primarily invented, developed, and formed by hackers – people experimenting out of curiosity and continually pushing the envelope on new technology (Hacktivist.com, 2001; Himanen, Castells, & Torvalds, 2001). However, in the last twenty years, beginning with negative media portrayals in movies such as *War Games*, the architects of yesteryear have become the risks of the future. As the public came to depend on interconnected information networks more and more over the past two decades, those with the potential to navigate the networks freely, and more importantly, those with the knowledge to reprogram these networks, increasingly found themselves vilified and stereotyped by the media and government.[7]

Much of the media's risk producing stems from actual, though abnormal, hacker attacks on the U.S. and its infrastructures during the late 1980s and 1990s (Freedman & Mann, 1997; Hafner & Markoff, 1995; Sterling, 1993). In general, hackers with a political agenda often target the U.S., its allies, and particular critical infrastructures attached to the Internet, in a form of political protest or opportunism.[8] The U.S. and those affiliated with the hegemonic power stand as prized targets. By virtually breaking into the U.S., one is capable of taking on the overwhelming world power on an individual level. Once again, in the virtual world "breaking in" is not synonymous with those lying outside the territorial U.S. invading, but even those present on U.S. territory, invading the power infrastructures that fuel hegemony. As concerns online politics, inside, outside, and other such territorial-based placements cease to exist.

Today, even with numerous corporations providing security software and repeated government crackdowns against hackers, hacking not only remains alive and well, but easier to partake in than ever before (Freedman & Mann, 1997; Himanen et al., 2001; Sterling, 1993). Documents such as "The Beginner's Guide to Hacking, Volumes I-III" proliferate and make it relatively easy for anyone with a networked computer to become

[7] Of course, looking at Ulrich Beck's theory of risk society this was to be expected. According to Beck, the media forges and shapes the risks in modern society more than anything else. With a flood of movies, television shows, and news reports displaying a hacker as a kid next door who – through a mysterious machine that most people do not understand the inner workings of – maintains an inconceivable amount of power to be destructive, society quickly came to regard hacking as a risk even though in general hacking has never lived up to its catastrophic potential.

[8] Attrition.org offers statistics on the number of verified attacks upon various states and institutions. Verification is produced when a hacker emails Attrition and tells them about a site defacement. Attrition then proves the hack by copying a picture of the defaced website and placing it on their website. For more information on this, see: http://www.attrition.org/mirror/attrition/country.html.

an independent political agent operating online. Tools that simplify the creation of a virus to the dragging of several icons across a computer monitor are available all over the Web. Numerous chatrooms operate as online classrooms, with hackers and "newbies" – people new to hacking – alike, discussing exploitable program glitches and swapping network passwords. Yet with all the danger that the proliferation of information such as this should present, particularly to international businesses relying heavily on communication networks, there are remarkably few reported incidences of colossal network breaches and damages. Like shark attacks, hacker break-ins are more an anomaly than an explicit political tactic.

Working alone, often for personal interests, issues of territoriality and scale are of little meaning or concern to online agents – it is gaining and maintaining interconnectivity to forbidden networks that is important (Freedman, 1997). Though the reasons behind hacking vary drastically depending on the individual, in stark contrast to many of the online anti-systemic movements, the philosophies behind hacking are generally not overtly political. In most cases, hacking stems from curiosity (Himanen et al., 2001), or as one hacker, Darklaser, responds when asked if he maintains a sense of purpose online, "looking to … have fun." Another hacker, K-Pax, notes, "[I hack] just for pleasure, no malicious [sic] intent involved, basically curiosity." Stinger believes that "challenge" drives his online actions, not necessarily agendas:

> "I normally hack for the challenge of it. It is fun. I don't really have any long term goal, I just do it for fun. But I don't really mess with nothing. It's not really cool to mess up peoples' [sic] comp unless you have a good reason."

Stinger goes on to explain that cinematic representations of hacker terrorists are somewhat embellished, because though such scenarios are theoretically possible, "Internet terrorists are really nonexistent because it takes [too much] effort to hack." It takes more than just curiosity and a connection to hack – it is a skill that is nurtured over time. K-Pax believes that "hacking is all about testing the system, finding the holes. It is a wonderful tool." When asked if he sees political uses for hacking he is more cautious: "yes, unfortunately [sic]… every tool has two uses, good and bad."

However, lest economics and politics be ruled out when it comes to hacking, those interviewed also illustrated the role that finance and power play in the underpinnings of hacking. As the hacker Phantom noted at one point:

> "It's ironic but I normally steal from the companies that I like. It's Adobe and Macromedia and companies like that that I end up stealing from, cause I really like their programs. I don't have thousands [of dollars] to blow on their software; so I'm gonna take it for free when I can."

Technophilia often truncates moral economic dilemmas – i.e., theft – amongst hackers, and in this way, hackers may symbolize more of a threat to free trade in the digital age than online organizations that simply protest and lobby against it. Hackers partake daily in a system of literal "free" trade – that is, property is not so much traded as acquired, reproduced, and given away for free. As Lightblader quipped: "[F]ree trade is cool." In the mind of hackers, the dispersing of information and knowledge goods to everyone helps equalize power in cyberspace.

Of course, this literal type of free trade goes against the very processes upon which hegemony depends. The U.S. needs exploitable trading practices to continue accumulating more capital from its position of economic advantage. In fact, as discussed in Chapter Two, one of the main benefits of privatizing the Internet was that it facilitated U.S. extra-territoriality, and therefore, yielded yet even more access for the U.S. to the global market. As the hegemony always desires, the Internet circumvented economic borders, facilitating an unprecedented fluidity of capital goods and finance. However, as the U.S. is now forced to modernize against, the Internet also allows for an unprecedented fluidity of non-state politics. Unimpeded, hackers and other online agencies – including many members of the everyday public, e.g., most college students – massively distributing and diffusing hacked information capital for free, threaten the vitality of the force driving the world-system and propelling the hegemony to power. Whether they realize it or not, hackers and persons trading digital music alike are active participants in online geopolitics.

Yet ironically, though hackers' actions speak otherwise, none of the hackers interviewed actually harbored any overt opposition to capitalism or globalization.  In fact, they were primarily concerned about the maintenance of competitive markets to help continue fueling technological development.  "I have nothing against Microsoft," Stinger noted, "but I do have a problem if they eliminate competition."  Phantom went on to note that he "love[s] capitalism," and that online technologies will only help capitalism remain more competitive, as long as "the big corporations don't [mess] everything up" by destroying smaller innovative companies.  Herein lies an interesting paradox – hackers are susceptible to, in fact have succumbed to, the prime modernity of mass consumerism, competitive markets, and neo-liberalism.  Rather than viewing themselves as inherently opposed to issues of globalization or unequal wealth distribution, they are in fact believers in it – needing capitalism to keep markets competitive so that there is always new technology to consume and play with.

If there is any underlying theme or political aspiration found in both the literature and interviews that might unite hackers, it is their quest to acquire and diffuse knowledge to the masses for free (Freedman, 1997; Hacktivist.com, 2001; Himanen et al., 2001; Ross, 1991; Sterling, 1993).  Like modern day Robin Hoods, hackers view information, and the knowledge that can be constructed from it, as the most valuable capital in the world-economy, and they are quite content to share any piece of the wealth they can get their keyboards on.  Furthermore, they harpoon against any restrictions on network access to the goldmines of information online, using such protections as a moral justification to hack.  As was discussed in Chapter Three, today many argue that information and knowledge have replaced labor and tangible goods as the most valuable capital and commodities of the world-system.  One look at the role of the service industry – primarily producing information and knowledge capital – in the U.S. economy, and the importance of these non-tangible products to the maintenance of the hegemony's economic position becomes apparent.

Borsook (2000) terms this motive of demanding access to and then freeing information and diffusing it, "technolibertarianism."  This philosophy was a recurrent topic amongst all the hackers interviewed. “Knowledge is power and the more knowledge you have the more power and sometimes [the] consequences [that] come with it,” Stinger mentioned. Later on in the interview he reiterated: “in cyberspace knowledge is power while in the physical world money and goods would be more important.” When questioned about information, Darklaser became quite emotive:

> “[Y]eah... that's the other thing[,] the democratization of information [sic] as opposed to [a] monopoly by colleges and stuff. [T]he idea that colleges have the 'correct' information[,] that they're the only ones authorized to distribute information[,] that's what happened mostly before the net. [T]hey had a lock on 'education' before the net[,] and then the best colleges and the most intelligent [teachers] are sometimes halfway around the world[,] and you couldn't get access to that info unless you flew there and/or attended the colleges[,] which you could only do if you were rich. [S]o in a sense [sic] the distribution of information is more democratic now [--] or rather more socialist.”

K-Pax concludes that “the internet is the greatest [sic] source of knowledge the world has ever known” and that “anything is possible here, …regulations are almost impossible.” Yet, of course, he feels that governments and corporations have a great interest in regulating and policing such intrusions into and thievery of their property.

Perhaps from ego, though more likely from the harsh reality of the network world, hacker responses to any mention of U.S. or international regulation are unilaterally condescending and disbelieving. Though reasons varied, there was unanimous accord that regulation of the Internet is “impossible” (Darklaser, K-Pax, NetGod, Phantom, Stinger, and Shroom). Some hackers could not even fathom why the U.S. would try to partake in such a colossal endeavor:

> Stinger: “I don't really think we have to worry about government regulation of the Internet. I really don't see why the government would have any interest in regulating the web...”

In Stinger’s mind it is a matter of simple economics – the costs of regulating the Internet far outweigh any potential benefits “and they still couldn’t have it all regulated.” When asked if something might induce cries for online regulation, such as a “digital Pearl

Harbor" scenario similar in impact to the attacks of 9-11, Stinger, perhaps naively, noted: "Well the attack would be against some government server or something; so they wouldn't need to regulate anything but their servers."

As discussed extensively throughout this thesis, however, the U.S. has every reason to regulate all "servers." The hegemony needs to maintain stability throughout the world-economy – including in cyberspace, where the most valuable capital is traded – in order to facilitate the most fluid accumulation of capital possible. The hackers are correct about one aspect of this regulation, however: due to geographic disparity, it is impossible for a territorial political entity to regulate the virtual network. In the last chapter it was noted that the United States is seeking to align itself with trans-national corporations to help in homeland defense. Though the costs are indeed high, the U.S. has already begun to fund the privatization of security – through the training of security experts – and the it is willing to acquiesce certain defense roles to the corporate world in order to maintain its position of dominance in the world-economy.

Other hackers, though anti-regulation, are not blind to the fact that the United States has been attempting to regulate the Internet for quite sometime now. They argue that the U.S. has met little success in achieving this goal, and that any future attempts by the hegemony to gain control of the virtual world will most likely fail as well:

> Darklaser: [I] think they tried and gave up. [I]t's as impossible as in the real world. [T]hey can't stop illegal immigration either. [P]eople who want to come in will find a way.
>
> K-Pax: Of course [the U.S.] will try [to regulate], they need their tentacles in everything. I don't think they will be able to. [T]he internet is anarchy. [A]nything is possible here, and regulations are almost impossible.

The assertion that the Internet is "anarchy" was repeated by several of the subjects (K-Pax, Phantom, and Shroom). It is of pertinence that the hacker outlook on network "anarchy" is nearly always positive, in opposite fashion to U.S. government policy perspectives on the same issue – as discussed in the previous chapter. Hacker reasoning abounds as to why contemporary governments are incapable of online regulation, but in the end, the answer to this enigma lies with geography.

The hegemony has always promoted the fluid movement of capital in the world-economy, deriving its power from open trade. Herein lies the double-edged sword for U.S. hegemony: while helping to develop the Internet into an open seaway for information and knowledge capital, no controls were put in place to prevent the fluid exchange of goods from slipping into "anarchy." United States power is inherently based on territorial concepts of sovereignty and, in overseeing the spread of the global network that is the contemporary Internet, the hegemony failed to consider the fact that it might eventually be incapable of regulating capital flowing through a networked geopolitical landscape. Thus, the conflict between hackers and the U.S. hegemonic order is really one of contrasting spatial outlook – whereas hackers view the anarchic network of cyberspace as liberating, useful, and continually evolving beyond any one person's or institution's control, U.S. agencies see it as an inadvertent risk to society and something that needs to be tamed through reflexive modernization.

Ironically, unlike the Federal agencies that are still attempting to police and prosecute, hackers have realized the root of the their advantage all along and continue to use geography to their benefit. When asked about government regulation, Darklaser cuts straight to the crux of the problem – territoriality: "Well the thing is... which government? A state government can only regulate the server in its country." Darklaser does not stop here in his analysis, noting that even if regulations were enacted, lack of territorial identity and affiliation on the Internet, as well as the continuous diffusion of information capital across the network, would complicate attempts at prosecution:

> "If you have stuff on a server which is illegal… who is responsible? The website provider? The user? What if the site allows uploads and someone uploads illegal stuff? It's a mess" (Darklaser).

K-Pax goes onto note that, as concerns U.S. regulation, there are "too [sic] many inlets. The [I]nternet is based off … the network structure. It breaks down a lot of barriers that our government tried to keep up." Darklaser believes that lack of territoriality in cyberspace does not make all regulation impossible, but the spatiality of regulation will have to change. Instead of by area, as classic geopolitics is inherently biased toward, regulation will only be possible in certain directions: “[Y]ou can stop people from coming in (or at least try to) but how do you stop people from going out to a foreign server?” Until the inter-state system realigns itself to this new geography – assuming that doing so is possible – even regulation by direction will remain up to sub-state actors (e.g., corporations).

Hackers realize, though perhaps not explicitly, that a lack of territorial affiliation plays a key role in the their ability to, not only navigate around the virtual world, but to avert certain everyday laws that function in the real world – i.e., theft and property destruction. They are more than willing to take advantage of a lack of control from above, as it allows them to fulfill their network curiosity and information diffusing agendas. Phantom notes that he would never steal in the real world, he is too scared, but in the virtual world he feels “free from the risk of being caught.” When asked if he has any moral issues with stealing thousands of dollars worth of software from his “favorite” corporations, he replies: “I’ll stop someday when I’m making money” (Phantom).

Though not geographers, when prodded to provide insight on U.S. government difficulties in regulating cyberspace, hackers cite explicitly spatial reasons. As Stinger espouses: “…the scale and complexity of the net it is not all in one spot. The servers are all over the world. It would take an incredible amount of time and money to regulate it.” Darklaser concludes that one of the problems for states is that the Internet is “a virtual reality with connections to this reality.” He and Stinger believe that the Net’s ability to circumvent borders is “part of” (Darklaser) the states’ problem. “Cyberspace is sort of a different world that deals strictly with information instead of solid objects,” Stinger notes. The Internet provides the advantage of “be[ing] able to communicate with people long distance instantly” (Stinger), and thus quickly mobilize, organize, and identify from and with many nodes in the network. As distance is not an issue in this virtual space, identification through proximity is of far less poignancy to online citizens than affiliation through moral or political views.

Furthermore, also unlike social organization in the territorial world, online communities offer a sort of anonymity not present in the physical realm – “It can be an advantage to not be seen or recognized” (Stinger). Though agreeing that the ephemeral quality of the Net provides certain advantages over activity in the real world, particularly the ability “to communicate with the rest of the world to solve practical problems that colleges never teach anyway,” Darklaser does not succumb to any of the utopian visions of online invincibility, noting that: “there is really no anonymity on the net... If someone wants to find you… I suppose they can.” Yet the fact remains, in the vast expanse of the network and with minimal territorial affiliation, the odds of being caught for online property theft or destruction remain slim. The network geography of cyberspace more easily allows individuals to partake in processes that would be impeded by certain established institutions and social constructions of territorial geopolitics.

The ability to communicate and interact with people across the world remains a strong and common theme amongst all online agents interviewed. Interaction unimpeded by time, distance, or outside interference – such as curfews, socially constructed borders, and increasingly, language differences – lies behind the usefulness of the Internet to all human organizations in general. However, as many non-government agencies are discovering, such geography also provides a definitive advantage to groups attempting to forge action around contemporary issues and societal risks, as well as overcome the hurdles of territorial power. This is a major development for social and non-state political movements, as the history of the current world-system, most such groups have succumbed to, and subsequently withered from, the territorial metageography (Taylor, 1991).

The regulation of individuals, such as hackers operating online, is difficult even in a territorial environment – preventing someone from deciding to break into a house is as difficult as thwarting an online attack. Thus, the political institution of the state has traditionally enforced regulations through the threat, and actual use, of violence on subjects located within its territorial sovereignty (Taylor & Flint, 2000, p. 31-39). Yet the scale of operations that multiple actors can achieve when organizing online from around the world easily overreaches the sovereignty of the territorial state – thus the threat of violence is compromised as a tool of consensus making. The hegemony, with its extra-territorial reach has more capability than any other state institution of enforcing rules through the threat of violence, but how to use "force" in the virtual world raises serious questions. With the most nodes into the cyberspace, the United States finds itself in a precarious position, particularly when it comes to regulating organizations that are global in scope, harbor anti-systemic agendas, and not affiliated with any territorial entity.

## Non-State Agencies Online: Deterritorialization and New Scales of Politics

Four anti-systemic and sub-politics organizations were interviewed for information on how they use the Internet in a political capacity, as well as their spatial perspectives of online conflict. The organizations participating in the study were given pseudonyms: the Feminist Confederacy; the Non-Profit Network; the Green Earth Movement; and the Socialist Front, the last of which represents a traditional anti-systemic movement, as compared to the first three groups, which will be considered sub-politics. Of these four entities, half of them did not exist prior to the advent of the Internet. The other two were real world non-state actors that began using the Internet as "more or less an extended tool in conjunction with all of our other tools in the real world" (Socialist Front). As will be shown, though use of the Internet varies extensively from organization to organization, in all cases the utilization of the Internet provides the movements a geographic and scalar advantage over state-based agencies.

All subject cases embrace a form of network organization online to which, as shown in the last chapter, the U.S. hegemony has been slow to modernize. Though organized in network fashion, these anti-systemic movements' and sub-politics' issues often hinged upon territorial consequences. This was quickly observable in an answer from one of the non-state actors studied, when they defined their "primary goal" as "socialism in our own country, and secondarily, socialism in the rest of the world" (Socialist Front). Though the issues fueling organizations into online action vary, in contrast to what was available to past social movements, the Internet offers a medium through which to act at the global scale (e.g., “We are part of a … worldwide movement.”).[9]

Though their methods vary slightly, all of the participating organizations use the Internet to facilitate operations in four vital procedural areas: communications, economics, organization, and mobilization. Furthermore, each organization views the Internet in opposite fashion to U.S. agencies, in a way that I will argue is geographically more pragmatic than state-based perspectives. By analyzing each of the four methods of use, it will become evident why online movements are confident that online activism will prevail over future regulation, commercialization, and other potential devolutions of the Internet stemming from U.S. and corporate pressures.

## The Network and Communication

Online movements have embraced the Internet for various reasons, but perhaps none so prominent as the medium’s ability to reach large audiences for minimal cost – the Internet “is faster [and] cheaper” (FC) than other methods. As the Socialist Front notes, the Internet is primarily used as “a mass PR instrument enabling [them] to reach far more people than [they] would in normal ways – [via] leaflets, books, radio programs, and the newspaper that [they] publish.” In particular, the World Wide Web is often used “very specifically to inform a lot of the politicians and a lot of people, especially … people” (SF) about issues of concern to the organization. The Non-Profit Network argues that “the [Net] is very effective in facilitating a method for many to speak out on issues they care about.” The Feminist Confederation sees it as a medium that is “excellent for raising awareness of an issue through news stories and action alerts; allowing feminists to communicate their policy preferences,” as well as “publicizing the organization” and

[9] Peter Taylor (1991) has argued that past social movements have often failed due to poor geographic strategy. Often times, social movements, such as Communism and socialism, succeed in attempting to take control of a territorial state. However, once they have control of this capitalist institution, they are still outnumbered by the states that are inherently opposed to the movements’ positions. Due to their position within a territorial state, such movements are often incapable of carrying the conflict to the global scale – the only scale at which they can change the system.

"encouraging individuals to take … action." In its most basic capacity, the Internet acts "simply as another medium of communication" (FC). It is, however, a medium of communication through which human agency can interact with, and influence, people around the world. More importantly, it is a medium that is not easily contained by the borders of state sovereignty – nor reined in by the current hegemonic order.

Much more than just being a tool to spread news, information, and alerts to members of online organizations, the Internet is also heavily used for reaching out to a "global community" (FC; NPN; SF) and recruiting. When asked about its place in cyberspace, the Socialist Front noted that it defined itself as

> "a part of the global community of people connected through cyberspace. If it weren't for cyberspace, [we] wouldn't be able to communicate with [certain] people. [We] wouldn't even know that they existed. [We] wouldn't know what they were doing. And being on the Internet and communicating on the Internet gives you a feeling of coexistence, of being together, even though you might not be linked together in the real world."

This process of global networking stands in direct contrast to the territorial organization of persons around proximity (e.g., township affiliation) and by nation (i.e., contiguous association through cultural similarities). As the Feminist Confederacy explains:

> "The Internet has been excellent at getting people who may have had a vague interest or personal attachment to an issue connected to regular expert (and quasi-expert) sources of information on that issue – including, for the first time, non-profit organizations."

Garnering support for online organizations, and the particular political issues that they stand for, appears to be done through consistent knowledge production: "Having our daily feminist news online and campaigning specific sites has allowed us to become established as experts on particular subjects, where that would be difficult to show otherwise [through conventional media]" (FC). In this way, people from different localities are capable of coalescing into online communities, through the sharing of information and experiences in the virtual world (Rheingold, 2000). In similar fashion to how the revolutionary technology of the printing press allowed states to forge identity around linguistic nations (Anderson, 1983), today's Internet is facilitating the development of networked virtual communities.

As Taylor and Flint (2000, p. 42-48) note, the scale of the nation-state has traditionally acted as a filter between the local and the global – shielding everyday life from the global economy. Its predominance over most people's daily life is why it is the scale most often at the center of human cognizance (e.g., national news, national sports, national weather, et cetera). However, Agnew laments that the social sciences – political science and international relations in particular – have ignored other scales and forms of geographic organization by almost exclusively focusing the nation-state when developing their theories (Agnew, 1994, 1998, 1999). He calls this state-centrism the "territorial trap," and argues that it threatens scientific cognition of many processes operating in the world-economy (Agnew, 1994, 1998, 1999). Today, however, the Internet provides a medium through which political institutions (e.g., households, curling fan clubs, et cetera) are capable of linking and cooperating at the global scale, above and beyond the filter of the nation-state and the vulgar restrictions of territorial proximity.

Thus, by snowballing and linking persons concerned with particular issues to relevant information and data, an online agency is capable of exponentially "expanding its base of activists" (FC), or participants in the community, as word and recognition spread through the global Internet.[10] Yet, while professing that they are attempting to forge "global communities" around particular issues, the eventual scale of impact from these organizations is often local. The Feminist Confederation remarks that the Net has been "excellent for recruiting … individuals to take local action." The Socialist Front notes that it "doesn't use the Internet locally as much as it would like to," but that this "will be the next step" in its conflict against "neo-liberal globalization." With the

[10] An example of this was provided by the Feminist Confederacy: "I like to think that after someone reads 10 articles on the terrible situation of women in Afghanistan, they'll want to email their Congress member; after they send 10 emails, they'll want to have their Girl Scout troop raise money for an underground school; after they raise $2000, they'll want to organize a fundraising event for all the Girl Scout troops in the state, etc. Whereas pre-Internet they may have read just [one] story in the newspaper and let [the issue] slide. Furthermore, the first wave of interest generated on the Internet is now frequently generating a second wave of interest in the mainstream media – e.g., www.HelpAfghanWomen.com -- finds its way onto CNN after tens of thousands of emails and faxes to the State Department for the last [five] years force Colin Powell to write Afghan women into the agenda for rebuilding Afghanistan."

Internet, online organizations are capable of organizing and galvanizing around particular nodes, localities, in the network. These communities, often anti-systemic movements and sub-politics, can mobilize, organize, interconnect, and accumulate capital within the world-economy through their nodal matrixes – something territorially fixed, immobile institutions cannot prevent and are having difficulty reflexively modernizing to.

## The Economics of Online Movements

As might be expected, much of the advantage to communicating and recruiting online stems from simple economics. As already mentioned, online activism, communication, and information dissemination is relatively cheap compared to other mediums and methods – "we can reach more people with fewer staff" (FC). However, though minimal, the costs of being in the virtual world do add up, and monetary support is perhaps even more vital than participation for online movements. Both the Socialist Front and the Feminist Confederation use the Internet to "raise donations for campaigns" (FC) and to "sell stuff" (SF). Conversely, Non-Profit Net is influenced by economics in the opposite manner, not using the Internet to collect money but also not daring to "engage in activity that [goes] against … our corporate sponsors." By supporting Non-Profit Net, corporations have power over some online sub-politics, capable of molding Non-Profit's agency and asserting influence over non-profit matters. No matter where income comes from, organizations are loath to utilize the Internet in any manner that may threaten the accumulation of capital. Just as in the real world, certain online conflicts and politics arise from the need to accumulate capital in order to gain better position in the world-economy.

The Socialist Front argues that "the big corporations still have the main advantage" over all other actors in cyberspace. Due to the fact that most search engines and network providers are corporate, the Internet is naturally becoming dominated by the capitalist rules of the real world. Several of the organizations – the Socialist Front and Feminist Confederation – expressed concern about the commercialization of cyberspace.

When asked to expand on the discussion of economic disparity online, an IT specialist at the Feminist Confederation lamented:

> "As it becomes increasingly standard to buy placement on search engines … and wherever links are present on the Internet, the less leverage we have compared to corporations online."

The possibility of being purposefully ignored by corporations maintaining vast amounts of power over the Internet – e.g., AOL's tactic of censoring anything it deems potentially offensive – is a real issue to online organizations. As one organization noted, "[c]orporate domination is a concern, particularly where it concerns search engines and other typical methods for users to find good information" (FC). Some of the online movements gripe that such developments defeat the purpose and vitality of the Internet. The Socialist Front showed the most consternation concerning its ability to use the Internet to the fullest potential:

> "We have to do a lot of footwork just to get our Internet site, you know, so that people know that you are there. It is not enough to just have a small link [on] Yahoo or on one of the other search engines. We need some kind of advertising that we can't afford."

The organization went on to complain that corporate takeover is "of course [an issue] … it's a problem if somebody starts owning the Internet, as it is a kind of organism that has to lead its own life" (SF). Finally, it was noted that regulations will probably come forth, "but they have to be for the good of the Internet … not just for the good of the corporations or governments [sic]" (SF).

Of course, such egalitarian regulations are unlikely, particularly if the U.S. follows the path of reflexively modernizing by acquiescing certain security powers to trans-national corporations. As discussed in the previous chapter, corporations comprise one of the few allies the U.S. can turn to in three key ways. First, they depend on the fluid and protected movement of capital just as much, if not more, than nation-states. Second, as political institutions they are already organized in a network fashion – something needed to fight networked adversaries such as sub-politics and anti-systemic movements (Arquilla & Ronfeldt, 1996, 1999c, 2001a, 2001b, 2001c). Finally, they own and operate a vast majority of the infrastructure upon which the Internet relies and depends. Though currently not a top economic priority for many corporations, as only a few specialized companies (e.g., Novell and McCaffee) stand to accumulate much capital from it, helping to secure information flows across the Internet will gain corporate backing if the U.S. should decide to start funding, and thus provide capital incentive, to such an alliance (CNN, 2002). What might develop from such a coalition between trans-national corporations and the United States is uncertain, but what can be counted on is that such a partnership will further attempt to control online political agency. Moreover, as discussed in Chapter Two, this hegemonic alliance will attempt to rein in any movements that go against the prime modernity and threaten the stability of the capitalist world-economy in particular.

No matter the case of current economic pressures, and future scenarios of U.S.-backed online corporate hegemony aside, for now the cyber-medium still provides by far the most cost effective method of global communication and organization (Anonymous, 1998; Arquilla & Ronfeldt, 1999; Cassel, 2000; Chroust, 2000; Himanen et al., 2001). As the Feminist Confederation noted:

> "[C]ompared to other media, which have always been 100% pay-for-placement – i.e. tv and radio commercials, newspaper ads – the Internet remains a superlative means of publicity for issues [and] organizations."

In fact, non-state actors in cyberspace are increasingly realizing that, unlike any previous technological development, which consisted of one-way or binary channels of communication, one of the Internet's prime assets at any price is its facilitation of multi-tiered organizing across international borders. Moreover, online organization can often lead to real world mobilization – nearly anywhere in the world.

## Organization and Mobilization

Organization and mobilization are the two areas where the network geography of the Internet ameliorates the territorial constraints imposed on non-state actors in the real world. Online movements tend to "view all Internet technology as a set of tools that each have their strengths and weaknesses for organizing" (FC). The Non-Profit Net "view[s] it as a very useful tool providing a reach that would not be possible utilizing other communication methods." The Green Earth Movement is more explicit, arguing that it

> "do[esn]'t see the Internet as a stand alone organizing tool, but it is good at certain things, in particular, moving information quickly between a large number of people, or gathering information from a large number of people."

Even with the advantages to organization that the Internet brings, the Feminist Confederation believes that "[m]aking a strong personal impression still requires personal interaction" and "[t]he Internet is particularly bad for getting across complex ideas, and allowing groups to refine complex ideas together." Yet the point is, the Internet is great for bringing persons from across a vast swath of territory together at a point, or as the Non-Profit Net sums up nicely: "reach[ing] people all over." Above and beyond *communication*, as alluded to previously, cyberspace allows the *organization* of political action within Taylor's (1981, 1987, 1991; Taylor & Flint, 2000, p. 42-48) scale of the world-economy, beyond the scale of the nation-state. It is this ability to bring human agencies together, regardless of their territorial placement in the real world, to unite and act together around a cause, that makes the network geography of the Internet so conducive to non-state political mobilization.

Online organizations use the Internet in a variety of different ways to mobilize for political action, but all of the methods share one common trait – they circumvent territorial controls. This is of particular importance for the growth and strength of sub-politics. The Internet "empowers" members of online movements by providing them "the sense that they can have a quick means to impact policy decisions, volunteer for a campaign, or [voice] what issues they think are most important" (FC). Tools such as bulletin boards, chat rooms, profiles, and various community software packages – some of which are developed by the organizations themselves (FC) – are "great for creating a sense of connection between individuals and activists, which helps invigorate a base of individuals who will take action on an issue when it arises" (FC). In other words, sub-politics can emerge, dynamically expand, and quickly evolve with ease in this network environment.

Many of the organizations voiced the belief that without the Internet, individuals were less likely to take action over certain political conflicts due to a lack of follow up information on an issue and the amount of effort it took to find an organization dealing with a specific issue: “pre-Internet [someone] might have read just 1 story in the newspaper [on a social issue] and let it slide” (FC). Now when irritated by something in the media, people are more likely to go online and uncover information on the issue relatively easily. They may even find a group concerned about the issue and join or participate in an organized, networked activity. This has proven particularly true for environmental movements, when people begin to realize that certain environmental issues are “begin[ning] to affect [their] actual locality” (GEM). Thus, as the U.S. reflexively modernizes to a plethora of societal risks – environmentalism, theft of information property, nuclear proliferation, et cetera – the Internet provides sub-politics a previously inconceivable opportunity to quickly develop and take action. It allows for increased mobility in fighting for certain issues, and facilitates the integration of different sub-politics fighting for similar causes.

As discussed earlier, once movements organize into a nodal network at the global scale, it becomes inherently difficult for state institutions, including the world hegemon, to stop them from using their deterritorialized structure to accumulate support for causes across international borders (e.g., the Chiapas of Mexico) and participate in politically motivated campaigns anywhere in the world. Online organizations have been aware of this advantage for sometime and, in general, do not believe that the U.S., or any other government for that matter, are capable of overcoming the hurdles to regulating the Internet. “The Internet will remain [viable] because it is built in this way – very, very, very hard to control” (SF).

Of even more interest than how easily these organizations have adapted to the network geography of cyberspace is how they visualize, philosophize, their use of this space. Though not asked specifically about geography, various spatial philosophies and perspectives arose from the organizations in their answers to the questionnaires. Though the Feminist Confederation noted that their organization does not visualize the Internet "as a space anymore than … the phone network," it went on to argue that the Internet "allows people to find a whole crowd of like-minded individuals, even if they're each isolated in their own geographical communities." Furthermore, the organization visualizes its use of the Internet as taking place "[around] the globe," and that because of the magnitude of the organization's reach, "the sense of being part of something larger is no doubt empowering and may serve as an impetus to act upon … political opinions" (FC). Thus, the scale and reach of the Internet is viewed as an advantage for all of the above discussed reasons: communication, economics, organization, and mobilization.

The Socialist Front and Green Earth Movement recognize that, though the structure of the Internet is powerful and empowering for their organization, the true benefits of online activism can be found in the agencies operating through the network and in how these processes interact with the real world. As the Socialists note:

> "The Internet is seen as a medium that has to interact with all the other stuff we're doing. We don't set out to do stuff on the Internet that we wouldn't be doing in real life, so … things that only exist virtually, online, wouldn't be of much interest to us. We use [the Internet] more or less as an extended tool in conjunction with all of our other tools in the real world."

As the above statement and this chapter have made quite obvious, for the most part online organizations currently use the Internet for communication, information dissemination, recruiting, and organization. Thus, its use is very much attached to what political events are occurring in the real world. However, as threat of government regulation and corporate intervention grows in cyberspace, and the technological capacity of the organizations continually increases, all of the organizations in this study envision a culminating battle between traditional powers (i.e., states and corporations) and new online politics (i.e., individuals and political movements operating in cyberspace) over various political issues. Subsequently, many believe their use of the Internet will change from how it is used today.

Though all of the organizations agreed to the statement that “[t]he Internet will remain” (SF), they also harbored different concerns about how it will evolve.  The Socialist Front and Green Earth Movement expressed concerns with both corporate domination and big brother scenarios:

> “The big corporations and the military, of course, that see the Internet as something that they invented and can control, will always try to get a grip on it and try to put in limitations for non-commercial uses.  And the government agencies, for one, would like a more big brother like Internet, for sure.  And they are trying every[thing] they can to get to that point.” (SF).

Whereas the Socialists see corporate “ownership” of the Internet as a problem – “we would protest against any regulations that would limit online opportunities” (SF) – they also recognize that eventually “there has to be some kind of regulations” (SF).  But Socialists went onto emphasize, in similar fashion to Lessig’s (2001) argument in *Foreign Policy*, that regulation must be well thought out, include the input of actors aside from the state, and not be based off of the reactionary ideas of ill informed politicians (SF).

The Feminist Confederacy is less concerned with attempts by states to regulate the Internet as “[w]e’re not doing anything on our sites outside of facilitating citizen communication with those in a position to change (political or corporate) policy.”  For the feminist organization, mobilization against Internet regulation would “depend on the particular reform.”  They go on to note that they would watch such regulatory measures carefully, and “[there] is no politically acceptable excuse in a democracy for limiting constituent access to representatives or to each other” (FC).  The Non-Profit Network notes that it “would not protest” against Internet regulation, because “it is not a concern” to the organization which does nothing illegal online.  However, though some of the organizations interviewed for this study do not find threat in government regulation, most statements uphold the belief that if attempts at cyber-regulation ever become excessively totalitarian, online sub-politics will be forged around this new risk to society and challenge any such reforms.

In general, online organizations see the Internet as democratizing politics and the media "by making it easy for organizers to harness the collective power of like-minded individuals" (FC). Other groups believe the Internet will begin being used by most people in the "industrialized world" and make it a particularly good tool for conflict in those regions, but they remain uncertain about the Internet's effectiveness in the periphery (SF) – where few people are networked and most infrastructure remains offline. Online organizations will likely "use the Internet much more offensively" in the near future and make it "a more integrated part of what [they] do" (SF). The Green Earth Movement believes that online action is bound to increase and become "a more viable and acceptable method of protest" (e.g., hacktivism and virtual sit-ins). The Socialists provide examples of how they see the Internet being used down the road:

> "[M]ore or less, the Internet will be connected to the real world more in the future. So that while we are on a demonstration, there will be online videocasts of the demonstration [and] of what goes on. There will be opportunities for others to participate virtually. And different kinds of meetings. Well, [we'll be] more integrated."

Perhaps because of this ability to integrate and evolve with the Internet, rather than need to reflexively modernize to it, unlike traditional adversaries of hegemonic powers, many online organizations do not dread conflict in virtual space. They are confident that they hold the upper hand against the U.S. and any other institutions attempting to politically control the Internet. The Socialists note that

> "I think [hacktivism and online movements] will remain on the Internet. It's a bit like when people attempt to copyright their music, or protect their films … [other] people will always find a way around it, and that will be the same with hacktivism. [We] use the Internet in a … way that if they try to put up barriers and obstacles, we'll figure a way to get around them. And maybe we will even get stronger [from this]. I don't think the governments will gain supremacy."

The Non-Profit Network, as well, sees online groups only becoming "more viable" in the future. To this end, the NPN organization's main aim is to help other groups utilize the

Internet. Even the Feminist Confederacy sounds an open call to all non-state actors with a political cause or moral issue to join network politics: “the next step is for activists and non-profits to keep working on ways to motivate this crowd of better-informed citizens to real-world action.”

## Conclusion

This chapter has shed light on the function and role of non-state agencies operating in cyberspace. By focusing on hacking and organizations with anti-systemic, sub-politics agendas, several interesting trends were discovered, all of which interrelate with hegemonic decline, reflexive modernization within risk society, and geography, or more particularly, the changing metageography of the world-system.

Today, hackers can be viewed in two lights, pending perspective: as a risk to society or as sub-politics. Those in power, the U.S. and corporations, have begun representing hacking as a risk of untold consequence to the security of anyone and everyone connected to the Internet. Though, the potential of rogue online agents sparking chaos on vital networks does exist, this risk is fueled more by the paranoid speculation on the part of political institutions, that stand to lose power from such a happenstance, than by real life experiences. From another vantage point, due to their very ability to push the hegemony and other institutions with power into a mode of reflexive modernization and risk inventing, hackers may more objectively be deemed a form of sub-politics. Their existence and agency is coercing institutions to modernize or be deemed irrelevant.

Though many hackers do have political agendas, in general hackers are not motivated by politics but rather curiosity and a different perspective of the world – what Himanen and Castells term “the Hacker Ethic” (Himanen, Castells, & Torvalds, 2001). They provide an alternative economic perspective to that of capital accumulation – capital diffusion. Ironically, perhaps due to the Internet’s development as part of prime modernity, hackers are not necessarily anti-systemic, and in fact, many whole-heartedly embrace the ideology of Americanization – that open markets and global competition are desirable for purposes of mass consumption. However, almost universally, hacking's main objective is to liberate information and knowledge capital from hegemonic control – be it a university, corporation, or the United States.

Hacker diffusion of this reproducible, and most valuable, knowledge capital is meant to spread wealth more equally. Whether it does is debatable – e.g., not many citizens of African states are connected to the network and capable of receiving this wealth – but the fact is that this anarchic distribution of capital threatens the role of territoriality upon which hegemony and the inter-state system rest. The hegemony promotes and benefits from more fluid lines of capital trading and exchange; however, an anarchic system of trading in a nodal network respecting no boundaries, between individuals nonetheless, threatens the role of the state in the world economy. Furthermore, this role change curtails the power of states, and thus, the world hegemon in geopolitics.

Thus, even though they participate in trading information and knowledge capital illegally, this is not anti-systemic per se. However, it is a form of sub-politics. Their ability to subvert online controls, institutions, and traditional regulations on the flow of capital goods is inherently threatening to the U.S. – which depends on free trade to extrapolate yet more surplus capital from the world-economy. Furthermore, the proliferation of hackers – anyone interested and connected to the Net can become a hacker with practice and time – allows people who wish to participate in the geopolitics of the world-economy an opportunity to confront more powerful political institutions.

Hackers are cognizant that it is the network structure – or geography – of the Internet that liberates them from the yoke of real world barriers to agency. They use the Internet as an appendage to their bodies to participate in economic and political activity at a global scale – above and beyond the control of any state, including the world hegemon. Thus, this group of individuals provides a prime example of the effects that the deterritorialization of geopolitics is having on the world-system. For the first time in the history of capitalism, the most powerful state in the world-economy is incapable of stopping an individual from effectively subverting its control and powers without threat of true repercussion.

The online organizations reviewed in this chapter represent a larger scope of sub-politics than hackers, and also included an anti-systemic movement. The Socialist Front is inherently anti-systemic, and uses the Internet to enhance its goals and aims. The three sub-politics groups – the Feminist Confederacy, the Green Earth Movement, and the Non-Profit Net – all sprout from various societal risks that current political institutions of the world-economy have failed to effectively stem. One similarity ties all four groups together – the use of the Internet's network geography for organization and mobility.

Online movements use the Internet in a variety of capacities, which have been broken down into four realms: communication, economics, organization, and mobilization. As for communication, the Internet provides the cheapest and fastest method for internal dialogues, external recruiting, spreading information to the masses, and integration of different branches of the movements. The ability to reach innumerable amounts of people, anywhere in the world, makes the Internet far superior to traditional, print and voice mediums, which depend on territoriality and point-to-point connection (i.e., airwave jurisdictions, newspaper distribution, and telephones that connect from node to node, rather than node to multiple-nodes). Thus, online organizations use the Internet to subvert territorial barriers to communication – a prime example of this is, of course, the Chiapas Movement of Mexico, but other examples proliferate on sites such as Indymedia.org.

The Internet has helped sub-politics and anti-systemic movements in the economic sphere of operations as well. Through the Internet, online movements are able to lobby for support, services, and funds from around the world. Though corporations admittedly have "an upperhand" (SF) online, and many of the movements fear that the corporate sector may eventually undermine their online recruiting ability through capitalist means – raising the price of placement on search engines, et cetera – the Internet still remains the most economic means for conducting operations.

Finally, and perhaps most importantly, the Internet has facilitated a network agency, whereby movements are capable of organizing in a nodal fashion and ephemerally, as well as mobilize into action quickly and without risk of retaliation. The Internet is now the primary avenue for sub-politics creation due to the fact that it facilitates the easy, and real time, congregation of the global community around any new risks that develop. Thus, the Internet is a superb infrastructure through which to force the reflexive modernization of political institutions and challenge various risks within society.

The implications of sub-politics and anti-systemic movements using the Internet in the above noted capacities are multiple. However, the origins of these implications can be defined as protruding from two areas: geography (both scale and deterritorialization) and the hegemonic cycle.

Today non-state actors finally have a tool that allows them to organize themselves above the scale of the state. The Internet allows individuals and organized movements alike, to integrate, disseminate, and communicate without the impediment of customs, controls, or borders. Using Christian bible smuggling as an example, whereas in the past religious subterfuge required sneaking bibles across controlled borders, often at the risk of arrest, today by posting the religious doctrine online, anyone connected to the virtual network is able to download it – borders are incapable of stopping this. This virtual mobility across the sovereignty of territorial states is of great importance to anti-systemic movements in that it broadens the scale of their conflict to one above the state, something that was difficult and rarely attainable in the past (Taylor, 1991). It has dire implications for the inter-state system, and the U.S. hegemon in particular, as it means that political sovereignty is quickly eroding in value as a control mechanism over political processes in the world-economy.

Concurrent with this deterritorialization of political geography, the United States is entering a period of hegemonic decline. No longer able to forge international consensus in the inter-state system, it needs to find new allies to maintain its power. Many of these new allies come from the trans-national corporate sector, as they too benefit from the prime modernity of mass consumerism. This blooming alliance between corporate and state powers is one of many processes leading to the creation of innumerable new risks in contemporary society – ecological, globalization, homogenization of cultures, et cetera – which in turn, fosters the development of sub-politics. The Internet, a technological innovation during the hegemonic cycle, is now a double-edged sword, used by sub-politics to fight risks that the hegemonic cycle has created.

The contemporary rapid growth of sub-politics using the Internet is forcing the U.S., which has inadvertently produced many of the risks, to reflexively modernize or eventually lose its position of power. Moreover, it forces this reflexive modernization much more rapidly than in the past, when state institutions and the hegemony held some power over the scale of sub-politics, and often successfully attempted to confine such movements to within a territorial area. As was discussed in the last chapter, reflexive modernization is not an easy process – expensive and extremely time consuming for a multi-tiered, hierarchical institution such as the U.S. Federal Government. If it fails to reflexively modernize to the numerous risks that sub-politics forge around, the U.S. hegemony will quickly begin to lose its position of power in the world-economy and the capitalist world-system will slip into crisis.

# Chapter Six: Conclusion

This thesis has illustrated how the Internet acts as a double-edged sword for United States hegemony. The current hegemonic headache of managing the negative impacts stemming from its own technological innovation, while benefiting from the extra-territoriality that this same innovation brings, is rooted in the United States' own spatial dementia, in that it is attempting to control a network geography through classic geopolitical means premised on territoriality. This chapter will bring the study to a close by summarizing the paramount theory, data, and analysis discussion that help answer the following questions posed in the Introduction:

- What role does territoriality play in U.S. hegemonic power?
- What are the implications of a changing metageography – from territorial to nodal network – on continued hegemony, and how is the U.S. reacting?
- What impingement do sub-politics and anti-systemic movements operating within a network geography have on a U.S. hegemony based on territoriality?

These problem statements will be succinctly answered by reviewing the United State's position in the hegemonic cycle; discussing the metageographic shift that is currently underway; noting hegemonic responses to decline and a changing metageography; contextualizing online sub-politics and anti-systemic movements; and by concluding with a discussion of the implications of this conflict between the territorial hegemony and online agencies.

The United States is currently in hegemonic decline. Though discussion varies over when exactly decline began, it can be agreed that it is entering the final phase of its cycle (Arrighi, 1994; Agnew, 1993; Flint, 2001; Taylor, 1996; Silver, 1999). Hegemonic decline is usually accompanied by global instability, as various powers – traditionally states – become more competitive and vie to better their position of power within the world-economy. This increased competition, coupled with less international consensus around U.S. policy, can be witnessed in numerous ways: e.g., increasing amounts of terrorist attacks on the United States; traditional allies disregarding U.S. diplomatic requests (Israel refusing to pull out of the West Bank in 2002); and in rising protest against the U.S. prime modernity of Americanization (i.e., globalization, suburbanization, and the culture of mass consumerism).

Unlike with past hegemonic cycles, the United States finds itself not only entering hegemonic decline but also confronting a potentially systemic evolution – a metageographic shift. As has been argued, global society is changing the way it organizes itself from territorial affiliation to a network of interconnected nodes. Beginning with the Treaty of Westphalia in 1648, the capitalist world-system has always organized itself territorially, with the political institution of the state using sovereignty to maintain its position of power over all other institutions by operating at the scale of the world-economy. By defending home markets, states are used to defend their national industries from outside dominance, while at the same time promoting their economies overseas for the accumulation of surplus capital. The hegemony is the state that dominates in production, trade, and finance, and with its economic leverage, promotes liberalism around the world in order to accrue yet more capital from exploitable markets. Thus, territoriality is an inherent necessity to *state hegemonic power*.

Today, however, the technological innovation of the Internet, in addition to fueling yet more capital accumulation for the hegemony, is also facilitating network organization across all scales of human agency. Moreover, the network metageography is not contained by the territorial borders of nation-states, as in a network it is always possible to circumvent around a border to connect to a node from another direction. As human agency begins to reorganize itself into networks, territorial states must reflexively modernize as institutions to the risks brought about by this societal change. The U.S. hegemony, in particular, stands to lose the most, as it must now face the costs and struggles of rapidly modernizing to the numerous risks stemming from this metageographic shift, while attempting to maintain its position of power within its withering geopolitical order.

The United States is currently reflexively modernizing to the risk of cyber-attack on its homeland and its inability to protect property rights of information and knowledge capital in cyberspace – the latter of which is a prime role of all world hegemons. However, as a territorially affiliated political institution, its policies and spatial perspective during this time of reflexive modernization are inherently, and repeatedly, tainted with a type of spatial dementia, based on territorial assumptions. Thus, again and again, the United States finds itself incapable of regulating cyberspace to a degree necessary for the stabilization of the current geopolitical order – protection of property and trade online, as well as political security. Its most likely avenue of reflexive modernization to the plethora of risks showering in from cyberspace appears to be acquiescing some of its power to trans-national corporations, which are often already organized in network structures, and may represent the only agencies capable of spanning the entire world-system due to their lack of territoriality. However, during this period of spatial dementia, when the United States experiments with policies of modernization, the Internet is increasingly being used by innumerable anti-systemic movements and sub-politics as a medium to bring their political conflicts to the global scale. Many of the risks and conflicts these groups clamor around are directly related to United States hegemony and its prime modernity, and thus, the United States finds itself at the center of many asymmetrical attacks by adversaries other than territorial nation-states.

Unlike past hegemonic transitions, when only nation-states competed against the hegemony for position advancement in the world-economy, contemporary anti-systemic movements and sub-politics represent part of the milieu of actors competing for power. By using the network space of the Internet to confront the hegemony, its geopolitical order, and the prime modernity at the scale of the world-economy, these agencies – from individual hackers to well organized political fronts – are capable of participating in international geopolitics. This ability for any political institution to participate in conflict at the scale of the world-economy, through the Internet, represents the beginning stages of the deterritorialization of geopolitics. Furthermore, this deterritorialization of geopolitics increasingly fuels the metageographic shift of society in general, as agencies begin to increasingly associate themselves around attributes other than territorial identity (e.g., political issues, religions, sexuality, interests, and various other types of virtual community building).

The implications of these developments on United States hegemony, and the world-system in general, are for the most part dire. Even excluding the deterritorialization of geopolitics being ushered in by the Internet, the world-system faces a long period of political conflict as the United States begins to lose its hegemonic might and states begin to compete for better position in the world-economy. Geohistorical analysis shows that when a hegemony begins to decline, it often resorts to reactionary measures and ideologies (for one example, see O'Tuathail's (1996, p. 75-100) critical analysis of MacKinder's heartland theory and its relation to British decline). The Bush Administration's creation of an Axis of Evil, as well as the building of a missile defense shield in an era of disarmament, illustrate that the U.S. is currently trying to reestablish a geopolitical order that has already slipped away from it.

Such policies that lust for the past hegemonic order of the Cold War will make effective reflexive modernization to the new realities and risks of deterritorialized geopolitics all the more difficult to achieve. In a vicious cycle, the hegemony is currently fueling its own spatial dementia to the realities of today's conflict by reverting to past, territorial based, strategies of success. Nonetheless, as Chapter Four illustrated, the U.S. is making progress in addressing homeland security from online attacks. However, rather than function as a panacea to U.S. hegemonic decline, the most likely modernization, an alliance with trans-national corporations, may symbolize an inescapable, quick slide to the end of U.S. power.

Geohistorical analysis illustrates that during decline hegemonies align themselves with regional partners to help maintain open seas for trade, because they no longer have the power to do it themselves (Arrighi, 1994; Arrighi & Silver, 1999). As reviewed in Chapter Two, eventually when systemic competition comes to a boiling point and results in global chaos, it is the hegemon that ends up waging the brunt of the war, and winds up receiving the brunt of carnage, while the junior partner primarily ensures the continuance of open trade and is far less affected (Arrighi, 1994; Arrighi & Silver, 1999; Taylor, 1993, 1996). Near the end of the systemic conflict, when all warring parties are bludgeoned and beleaguered, the junior partner joins the conflict and ends it decisively (Arrighi, 1994; Arrighi & Silver, 1999; Taylor, 1993, 1996). Thereafter, it is the partner that forges the new geopolitical order and rises to the role of hegemony (Arrighi, 1994; Arrighi & Silver, 1999; Taylor, 1993, 1996).

Today information and knowledge have replaced tangible goods as the most valuable capital in the world-system. The networks of the virtual world function as the seas of yesteryear – the paths through which trade and commerce are conducted. In asking corporations to ensure the protection and openness of the Internet, the U.S. strategy for reflexive modernization is really one of asking global corporations to become a junior partner (Arrighi, 1994; Arrighi & Silver, 1999). As anti-systemic movements and sub-politics confront the U.S. during this period of hegemonic decline, the United States will find itself in an expensive war against multiple, non-territorial movements – movements that, when lacking territorial affiliation, are labeled by the hegemony as "terrorists." No matter the issue, from radical Islam to radical feminism, by their very existence and immunity from U.S. regulatory power, all agencies using the networked virtual world are participating in the hegemonic decline of the United States.

Unlike past global conflicts deciding the outcome of hegemonic decline, much of this war between deterritorialized institutions and the hegemony will be played out on the Internet, fought over, and with, information and knowledge instead of traditional tangibles – tanks and bombs. Fortunately for the United States, no matter the number of, and real world violence stemming from, these online sub-politics and anti-systemic movements, geohistorical analysis illustrates that the hegemony always comes out on the victorious side of such global wars. However, there is one major distinction; the hegemony survives the conflict to become a junior partner to its former ally, which in turn has risen as the new world hegemon. The ascension of networked trans-national corporations to hegemony, or what Taylor (1996, p. 186-187) terms "ultra-hegemony," will symbolize the culmination and completion of the geopolitical deterritorialization that began with today’s online sub-politics.

# Bibliography

Adams, P. C., & Warf, B. (1997). Introduction: cyberspace and geographical space. *The Geographical Review*, *87*(2), 139-145.

Agnew, J. (1993). The United States and American Hegemony. In P. J. Taylor (Ed.), *Political Geography of the Twentieth Century: A Global Analysis* (pp. 207-238). New York: Halsted Press.

Agnew, J. (1994). The territorial trap. *Review of International Political Economy, 1*(1), 53-80.

Agnew, J. (1998). *Geopolitics: Re-visioning World Politics*. New York: Routledge.

Agnew, J. (1999). Mapping Political Power Beyond State Boundaries: Territory, Identity, and Movement in World Politics. *Millennium: Journal of International Studies, 28*(3), 499-521.

Agnew, J., & Corbridge, S. (1995). *Mastering Space: Hegemony, Territory and International Political Economy*. New York: Routledge.

Amin, S., Arrighi, G., Frank, A. G., & Wallerstein, I. (1990). *Transforming the Revolution: Social Movements and the World-System*. New York: Monthly Review Press.

Anderson, B. (1983). *Imagined Communities: Reflections on the Origins and Spread of Nationalism*. London: Verso.

Anderson, C. (2001). Is Japan still the future? *Wired, 9,* 117.

Anderson, R. H. (Ed.). (1999). *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*. Santa Monica, CA: RAND.

Anonymous. (1997). *Transforming Defense: National Security in the 21st Century*, [Website]. National Defense Panel. Available: http://www.fas.org/man/docs/ndp/front.htm [2002, Jan 23].

Anonymous. (1998). *Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses: Proceedings Report*, [Online PDF]. Potomac Institute for Policy Studies. Available: http://www.potomacinstitute.com/pubs/cyber.pdf [2002, Jan 22].

Anonymous. (1999). *ANSER Annual Report*. Arlington, VA: ANSER Corporation.

Anonymous. (2000, October 27, 2000). *Microsoft acknowledges theft of source code* (Webpage). New York Times. Available: http://www.nytimes.com/aponline/technology/27MICROSOFT.html [2000, October 27].

Anonymous. (2001). *Information Assurance and Critical Infrastructure Protection: a Federal Perspective (White Paper)*, [Online PDF]. GEIA [2002, Jan 19].

Anonymous. (2002a). *ANSER History*, [Web page]. ANSER. Available: http://www.anser.org/aboutanser/history.htm [2002, Dec 15].

Anonymous. (2002b). *ANSER Vision*, [Web page]. ANSER. Available: http://www.anser.org/aboutanser/ [2002, Feb 15].

Anonymous. (2002c, Jan 11). *Homeland Security Newsletter*, [HTML email]. ANSER [2002, Jan 11].

Anonymous. (2002d). *Improving National Security*, [Web page]. RAND Corporation. Available: http://www.rand.org/about/ffrdc.research.html [2002, Jan 28].

Anonymous (2002e). Novak, Hunt, and Shields. In CNN (Producer).

Anonymous. (2002f). *RAND's History*, [Web page]. RAND. Available: http://www.rand.org/history/ [2002, Jan 28].

Anonymous. (2002g). The world according to Tom Ridge. *Wired, 10,* 50-51.

Arquilla, J., & Ronfeldt, D. (1996). *The Advent of Netwar*. Santa Monica, CA: RAND.

Arquilla, J., & Ronfeldt, D. (1999a). The advent of netwar. *Studies in Conflict and Terrorism, 22,* 193-206.

Arquilla, J., & Ronfeldt, D. (1999b). *The Emergence of Noopolitik: Toward an American Information Strategy*. Santa Monica, CA: RAND.

Arquilla, J., & Ronfeldt, D. (1999c). Networks, Netwar, and Information-Age Terrorism. In I. O. Lesser & B. Hoffman & J. Arquilla & D. Ronfeldt & M. Zanini & B. M. Jenkins (Eds.), *Countering the New Terrorism* (pp. 39-84). Santa Monica, CA: RAND.

Arquilla, J., & Ronfeldt, D. (2001a). Fighting the network war. *Wired, 9,* 148-151.

Arquilla, J., & Ronfeldt, D. (2001b). Networks, netwars, and the fight for the future. *First Monday, 6*(10), Online: http://firstmonday.org/issues/issue6_10/ronfeldt/index.html.

Arquilla, J., & Ronfeldt, D. (2001c). Osama bin Laden and the advent of netwar. *New Perspectives Quarterly, 18*(4), Available only online: http://www.digitalnpq.org/archive/2001_fall/osama.html.index.html.

Arrighi, G. (1994). *The Long Twentieth Century*. New York: Verso.

Arrighi, G., & Sliver, B. (Eds.). (1999). *Chaos and Governance in the Modern World System*. Minneapolis: University of Minnesota Press.

attrition.org. (2001, May 17). *Attrition Defacement Statistics,* [Web page]. Available: http://www.attrition.org/mirror/attrition/country.html [2001, Sep 3].

Auerbach, J., & Bulkeley, W. (2000, February 10). Web in modern age is arena for activism, terrorism, even war. *The Wall Street Journal* [Electronic Edition].

Baker, D. (1998, Nov-Dec). The computer-driven productivity boom. *Challenge, 41*(6), 5-8.

Balsamo, A. (1995). Forms of Technological Embodiment: Reading the Body in Contemporary Culture. In M. Featherstone & R. Burrows (Eds.), *Cyberspace/ Cyberbodies/Cyberpunk: Cultures of Technological Embodiment* (pp. 215-237). Thousand Oaks, CA: Sage Publications.

Baran, P. (1964). *On Distributed Communications: Introduction to Distributed Communications Network,* [Website]. RAND Corporation. Available: http://www.rand.org/publications/RM/RM3420/ [2002, Jan 28].

Barlow, J. P. (1996, September). The netizen: the powers that were. *Wired, 4,* 53-56, 195, 197, 199.

Bauman, Z. (1999). *In Search of Politics*. Stanford: Stanford University Press.

Beck, U. (1992). *Risk Society* (M. Ritter, Trans.). Newbury Park, CA: SAGE Publications, Ltd.

Berry, B. (Ed.). (1976). *Urbanization and Counterurbanization* ( Vol. 11). Beverly Hills, CA: Sage.

Bodow, S. (2001, September). The money shot. *Wired, 9*, 86-97.

Borsook, P. (2000). *Cyberselfish*. New York: PublicAffairs.

Brandenburger, A., & Stein, E. (year unknown). *The Work of John von Neumann (1903-1957)*, [Web page]. Yale University. Available: http://mayet.som.yale.edu/ coopetition/vN.html [2002, Feb 2].

Brunn, S. D. (1999). A Treaty of Silicon for the Treaty of Westphalia?  New Territorial Dimensions of Modern Statehood. In D. Newman (Ed.), *Boundaries, Territory, and Postmodernity* (pp. 106-131). Portland, OR: Frank Cass.

Brzezinski, Z. (1998). *The Grand Chessboard*. New York: BasicBooks.

Buchan, G. (1996). *Information War and the Air Force: Wave of the Future? Current Fad?*, [Webpage]. RAND. Available: http://www.rand.org/publications/IP/IP149 [2002, Jan 30].

Burrows, R. (1997). Virtual Culture, Urban Social Polarisation and Social Science Fiction. In B. D. Loader (Ed.), *The Governance of Cyberspace* (pp. 38-45). New York: Routledge.

Cassel, D. (2000). *Hacktivism in the cyberstreets*. Alternet.org. Available: http://www. alternet.org/story.html?StoryID=9223 [2000, Oct 18].

Castells, M. (2000). *The Rise of the Network Society* (2nd Ed. ed.). Malden, MA: Blackwell Publishers, Inc.

Chroust, P. (2000). Neo-Nazis and Taliban on-line: anti-modern political movements and modern media. *Democratization, 7*(1), 102-118.

Cilluffo, F. J. (2000). Cyber attack: the national protection plan and its privacy implications, [Webpage]. *Journal of Homeland Security*. Available: http://www.homelandsecurity.org/journal/Articles/Cilluffo.htm [2002, Jan 22].

Cilluffo, F.J., Collins, J. J., Borchgrave, A. d., Goure, D., & Horowitz, M. (2000). *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies*, [Online PDF]. CSIS. Available: http://www.csis.org/homeland/reports/defendamer21stexecsumm.pdf [2002, Jan 19].

Clark, N. (1995). Rear-View Mirrorshades: the Recursive Generation of the Cyberbody. In M. Featherstone & R. Burrows (Eds.), *Cyberspace/Cyberbodies/Cyberpunk: Cultures of Technological Embodiment* (pp. 113-133). Thousand Oaks, CA: Sage Publications.

CNN. (2000). *U.S. spy chief: cyberspace a potential battlefield* (CNN.com), [Internet News]. Reuters. Available: http://www.cnn.com/2000/TECH/computing/10/17/tech.internet.security.reut/index.html [2000, Oct 17].

CNN. (2001). *Bush signs antiterrorism bill into law*. CNN.com. Available: http://www.cnn.com/2001/US/10/26/rec.bush.antiterror.bill/index.html [2001, Oct 28].

CNN. (2002). *U.S. Government Trains Cyberdefenders,* [Webpage]. CNN.com. Available: http://www.cnn.com/2002/TECH/industry/03/31/cyber.corps.ap/index.html [2002, Apr 1].

Cohen, E. A. (2002). The Anser Institute for Homeland Security. *Foreign Affairs, 81*(1), http://foreignaffairs.org/Search/document.asp?i=20020101FABOOK20026496.XML [2002, Jan 17].

Cox, R. W. (1981). Social forces, states, and world orders: beyond international relations theory. *Millennium, 10*, 126-155.

Crang, M. (1997). Analysing qualitative materials. In R. Flowerdew & D. Martin (Eds.), *Methods in Human Geography* (pp. 183-196). Harlow: Longman.

Creswell, J. W. (1998). *Qualitative Inquiry and Research Design*. Thousand Oaks, CA: Sage Publications.

Darklaser. (Pseudonym). Chatroom interviews, Jan & Feb 2002.

Davies, P. (1970). The American Heritage Dictionary of the English Language (p. 820). New York: Dell Publishing Company, Inc.

de Borchgrave, A., Cilluffo, F. J., Cardash, S. L., & Ledgerwood, M. M. (2000). *Cyber Threats and Information Security: Meeting the 21st Century Challenge,* [Online PDF]. CSIS. Available: http://www.csis.org/homeland/reports/ cyberthreatsandinfosec.pdf [2002, Jan 19].

Dillman, D. A. (2000). *Mail and Internet Surveys: the Tailored Design Method* (2nd ed.). New York: John Wiley and Sons.

Dorobek, C. J. (2001). *DOD envisions virtual Pentagon*, [Webpage]. Federal Computer Week. Available: http://www.fcw.com/fcw/articles/2001/1029/web-pent-10-30-01.asp [2002, Jan 24].

Earickson, R., & Harlin, J. (1994). *Geographic Measurement and Quantitative Analysis*. New York: Macmillan College Publishing Company.

Elwood, S. A., & Martin, D. G. (2000). "Placing" interviews: location and scales of power in qualitative research. *Professional Geographer, 52*(4), 649-657.

Everard, J. (2000). *Virtual States: the Internet and the Boundaries of the Nation-state*. New York: Routledge.

FC (Feminist Confederation). (Pseudonym). Online questionnaire and interview, Jan & Feb 2002.

Featherstone, M., & Burrows, R. (1995). Cultures of Technological Embodiment: An Introduction. In M. Featherstone & R. Burrows (Eds.), *Cyberspace/Cyberbodies/ Cyberpunk: Cultures of Technological Embodiment* (pp. 1-19). Thousand Oaks, CA: Sage Publications.

Fisher, U. (2001). Information age state security: new threats to old boundaries, [Webpage]. *Journal of Homeland Security*. Available: http://www. homelandsecurity.org/journal/Articles/fisher.htm [2002, Jan 22].

Fitting, P. (1991). The Lessons of Cyberpunk. In A. Ross & C. Penley (Eds.), *Technoculture* (pp. 295-315). Minneapolis: University of Minnesota Press.

Flint, C. (2000). The Geopolitics of Laughter and Forgetting: A World-systems Interpretation of the Post Modern Geopolitical Condition. *Geopolitics, Forthcoming*, 23 pages.

Flint, C. (2001). Right-wing resistance to the process of American hegemony: the changing political geography of nativism in Pennsylvania, 1920-1998. *Political Geography, 20*, 763-786.

Frank, D. (2001a). *Clarke presses industry on security*, [Webpage]. Federal Computer Week. Available: http://www.fcw.com/fcw/articles/2001/1203/web-clarke-12-05-01.asp [2002, Jan 24].

Frank, D. (2001b). *GovNet's fate hangs on policy*, [Webpage]. Federal Computer Week. Available: http://www.fcw.com/fcw/articles/2001/1210/pol-govnet-12-10-01.asp [2002, Jan 31].

Freedman, D. H., & Mann, C. C. (1997). *At Large: The Strange Case of the World's Biggest Internet Invasion*. New York: Touchstone Publishing.

Froehling, O. (1997). The cyberspace "war of ink and Internet" in Chiapas, Mexico. *The Geographical Review, 87*(2), 291-307.

Garamone, J. (2001). *Center works to protect communications infrastructure*, [Webpage]. American Forces Information Service. Available: http://www.defenselink.mil/news/Nov2001/n11072001_200111072.html [2002, Jan 24].

GEM (Green Earth Movement). Online questionnaire, Mar 2002.

George, P. (1998). *Dr. Strangelove: or How I Learned to Stop Worrying and Love the Bomb*. New York: Barnes and Noble.

Gibson, W. (1984). *Neuromancer*. New York: Ace.

Gibson, W. (2001, September). My Own Private Tokyo. *Wired, 9*, 117-119.

Gill, B. (1996). *China and the Revolution in Military Affairs*. Carlisle, PA: Strategic Studies Institute.

Goldberg, A. (1999, May 1999). The dangers of "hacktivism". *Upside, 11*, 38.

Graham, S. (1998). The end of geography or the explosion of place? Conceptualizing space, place and information technology. *Progress in Human Geography, 22*(2), 165-185.

Gramsci, A. (1971). *Selections from the Prison Notebooks of Antonio Gramsci* (Q. Hoare & G. N. Smith, Trans.). New York: International Publishers.

Gray, C. S. (1988). *The Geopolitics of Super Power*. Lexington: The University Press of Kentucky.

Gray, C. S. (1999). *Modern Strategy*. New York: Oxford University Press, Inc.

Hacktivist.com. (2001). *Hackers versus crackers*. Available: http://www.thehacktivist.com/article.php?sid=103&mode=thread&order=0 [2001, Oct 12].

Hafner, K., & Markoff, J. (1995). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Touchstone.

Haraway, D. (1991). The Actors are Cyborg, Nature is Coyote, and the Geography is Elsewhere: Postscript to 'Cyborgs at Large'. In C. Penley & A. Ross (Eds.), *Technoculture* (pp. 21-26). Minneapolis: University of Minnesota Press.

Haraway, D., Penley, C., & Ross, A. (1991). Cyborgs at Large: Interview with Donna Haraway. In C. Penley & A. Ross (Eds.), *Technoculture* (pp. 1-20). Minneapolis: University of Minnesota Press.

Hartigan, P. (1999, Jan 24). They call it 'hacktivism'. *Boston Globe*, p. 1.

Harvey, D. (1987). The world systems theory trap. *Studies in Comparative International Development*, *22*(1), 42-47.

Heilemann, J. (2001, June). Andy Grove's Rational Exuberance. *Wired*, *9*(6), 137-147.

Himanen, P., Castells, M., & Torvalds, L. (2001). *The Hacker Ethic*. New York: Random House.

Holloway, J. (2000). Institutional geographies of the new age movement. *Geoforum*, *31*, 553-565.

Holloway, S. L., & Valentine, G. (2001). Placing cyberspace: processes of Americanization in British children's use of the Internet. *Area*, *33*(2), 153-160.

Hopper, D. I. (2002). *House passes computer security bill aimed at thwarting hackers*, [Web page]. Associated Press. Available: http://www.nandotimes.com/technology/story/244182p-2315770c.html [2002, Feb 10].

Hudson, A. (2000). Offshoreness, globalization and sovereignty: a postmodern geo-political economy? *Transactions of the Institute of British Geographers*, 269-283.

Hugill, P.J. (1999). *Global Communications Since 1844: Geopolitics and Technology.* Baltimore, MD: Johns Hopkins University Press.

K-Pax. (Pseudonym). Chatroom interview, Feb 2002.

Kellner, D. (1995). Mapping the Present from the Future: from Baudrillard to Cyberpunk, *Media Culture*. London: Routledge.

Kennedy, P. (1988). *The Rise and Fall of Great Powers*. New York: Random House.

Keohane, R. O. (1984). *After Hegemony*. Princeton, N.J.: Princeton University Press.

Kitchin, R. M. (1998). Towards geographies of cyberspace. *Progress in Human Geography, 22*(3), 385-406.

Koch, L. Z. (2001). *It's time to stuff the cyber-nonsense*. thehacktivist.com. Available: http://www.thehacktivist.com/article.php?sid=150 [2001, Nov 24].

Koerner, B. I. (2000). *To heck with hactivism*. salon.com. Available: http://salon.com/tech/feature/2000/07/20/hacktivism/index.html [2000, October 18].

Larsen, R. J., & David, R. A. (2000). Homeland defense: assumptions first, strategy second, [Webpage]. *Journal of Homeland Security*. Available: http://www.homelandsecurity.org/journal/Articles/article1.htm [2002, Jan 25].

Latour, B. (1993). *We Have Never Been Modern* (C. Porter, Trans.). Cambridge: Harvard University Press.

Latour, B. (1998). *On Actor-network Theory: A Few Clarifications 1/2*. Centre for Social Theory and Technology, Keele University, UK. Available: http://www.tao.ca/fire/nettime/old/4/0071.htm [2000, June 20].

Latour, B. (1999). On Recalling ANT. In J. Law & J. Hassard (Eds.), *Actor Network Theory and After*. Malden, MA: Blackwell.

Lemos, R. (2001). *The cyberterrorism czar: what's next?*, [Webpage]. CNET News. Available: http://news.com.com/2008-1082-275751.html?legacy=cnet [2002, Jan 24].

Lenk, K. (1997). The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing. In B. D. Loader (Ed.), *The Governance of Cyberspace* (pp. 126-135). New York: Routledge.

Lessig, L. (2001). The Internet under siege. *Foreign Policy*(127), 56-65.

Lindsay, J. M. (1997). *Techniques in Human Geography* . New York: Routledge.

Loader, B. D. (1997). The Governance of Cyberspace. In B. D. Loader (Ed.), *The Governance of Cyberspace* (pp. 1-19). New York: Routledge.

LoBaido, A. C. (1999). *The Beijing hack attack: Hong Kong-based cyber warriors build anti-China techno army*. WorldNetDaily.com. Available: http://www.infowar.com/hacker/99/hack_122299c_j.shtml [2000, Oct 18].

Luke, T. W. (1998). Running Flat Out on the Road Ahead: Nationality, Sovereignty, and Territoriality in the World of the Information Superhighway. In G. O'Tuathail & S. Dalby (Eds.), *Rethinking Geopolitics* (pp. 274-294). New York: Routledge.

Luttwak, E. N. (1992). The U.S.-Japanese crisis. *Washington Quarterly, 15*(4), 111-118.

Mann, M. (1997). The Autonomous Power of the State. In J. Agnew (Ed.), *Political Geography, A Reader* (pp. 58-81). New York: John Wiley & Sons, Inc.

Marden, P. (1997). Geographies of dissent: globalization, identity, and the nation. *Political Geography, 16*(1), 37-64.

Martin, M. (1998). The Culture of the Telephone. In P. D. Hopkins (Ed.), *Sex/Machine: Readings in Culture, Gender and Technology* (pp. 50-74). Bloomington: Indiana University Press.

Marston, S. A. (2000). The social construction of scale. *Progress in Human Geography, 24*(2), 219-242.

McCullagh, D. (2002, March). Richard Clarke is Ready for a Fight. *Wired, 10,* 104-111.

Messmer, E. (2000). *U.S. Army kick-starts cyberwar machine,* [Web page]. CNN.com. Available: http://www.cnn.com/2000/TECH/computing/11/22/cyberwar.machine.idg/index.html [2000, Nov 22].

Modelski, G. (1987). *Long Cycles in World Politics*. Seattle: University of Washington Press.

Molander, R. C., Riddile, A. S., & Wilson, P. A. (1996). *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: RAND/National Defense Research Institute.

Mulvenon, J. (1999). The PLA and Information Warfare, *The People's Liberation Army in the Information Age* (pp. 175-186). Santa Monica, CA: RAND.

Mitchell, W. J. (1999). *E-topia*. Cambridge, MA: MIT Press.

Nakamura, L. (2000). "Where do you want to go today?"  Cybernetic tourism, the Internet, and transnationality. In B. E. Kolko & L. Nakamura & G. B. Rodman (Eds.), *Race in Cyberspace* (pp. 15-26). New York: Routledge.

Neeley, D. (2000, February). Hacktivism or vandalism? *Security Management, 44*, 30.

NetGod. (Pseudonym). Chatroom interview, Jan 2002.

Newman, C. (2000, Sep 12). Cyber-security called 'dismal': House panel warns federal data is vulnerable to hackers. *The Washington Post* [Electronic Ed.].

NPN (Non-Profit Network). (Pseudonym). Online questionnaire and interview, Feb & Mar 2002.

Oberhauser, A. (1997). The home as "field": households and homework in rural Appalachia. In J. P. J. III & H. Nast & S. Roberts (Eds.), *Thresholds in Feminist Geography* (pp. 165-182). Lanham, MD: Rowman and Littlefield.

O'Tuathail, G. (1996). *Critical Geopolitics*. Minneapolis: University of Minnesota Press.

O'Tuathail, G. (1998). Deterritorialized threats and global dangers. *Geopolitics, 3*(1), 17-31.

O'Tuathail, G., & Dalby, S. (Eds.). (1998). *Rethinking Geopolitics*. New York: Routledge.

Oppenheim, A. N. (1992). *Questionnaire Design, Interviewing, and Attitude Measurement* (New Ed.). New York: St. Martin's Press.

Parker, G. (2001). An Uneasy Relationship: Geography and Politics at the Turn of the Millennium. *Political Geography, 20*, 120-126.

Phantom. (Pseudonym). Interview, Dec 2001.

Poster, M. (1995). Postmodern Virtualities. In R. Burrows & M. Featherstone (Eds.), *Cyberspace/Cyberbodies/Cyberpunk* (pp. 79-95). Thousand Oaks, CA: Sage Publications.

Price, D. (2000, August 14). Pentagon recruits hackers: experts say hiring them could compromise security and encourage criminal behavior. *Detroit News* [Electronic Ed.].

Radcliff, D. (2000). *Inside the world of a 'hactivist'* (CNN.com). Computerworld [2000, Oct 18].

Rheingold, H. (1995, March-April). Virtual community. *Utne Reader,* 61-64.

Rheingold, H. (2000). *The Virtual Community: Homesteading on the Electronic Frontier* ( Revised ed.). Cambridge, MA: MIT Press.

RIA. (2000). *Russian computer crime wizards pose real danger*. infowar.com. Available: http://www.infowar.com/hacker/00/hack_101200d_j.shtml [2000, Oct 18].

Ronfeldt, D., Arquilla, J., Fuller, G. E., & Fuller, M. (1998). *The Zapatista Social Netwar in Mexico*. Santa Monica, CA: RAND Arroyo Center.

Rosecrance, R. (1996). The rise of the virtual state. *Foreign Affairs, 75*(4), 45-61.

Ross, A. (1991). Hacking Away at the Counterculture. In C. Penley & A. Ross (Eds.), *Technoculture* (pp. 107-134). Minneapolis: University of Minnesota Press.

Salant, P., & Dillman, D. (1994). *How to Conduct Your Own Survey*. New York: John Wiley & Sons, Inc.

Sassen, S. (1991). *The Global City: New York, London, Tokyo*. Princeton, New Jersey: Princeton University Press.

Sassen, S. (1994). *Cities in a World Economy*. Thousand Oaks, CA: Pine Forge Press.

Sassen, S. (1998). *Globalization and Its Discontents*. New York: The New Press.

Schattschneider, E. E. (1960). *The Semi-Sovereign People*. Hinsdale, IL: Dryden.

Schwartz, J. (11/3/2000). Hacker defaces pro-Israel Web site as the mideast conflict expands into cyberspace. *NY Times* [Washington Ed.], Sec. A, p. 17.

SF (Socialist Front). (Pseudonym). Online questionnaire and interview, Jan & Feb 2002.

Sherman, S. (1999). Hegemonic transitions and the dynamics of cultural change. *Review, 22*(1), 87-117.

Shroom. (Pseudonym). Chatroom interview, Jan 2002.

Siano, B. (year unknown). *Just who WAS Dr. Strangelove, really?*, [Website]. alt.movies.kubrick (Web version). Available: http://www.krusch.com/kubrick/ Q06.html [2002, Feb 2].

Sieberg, D. (2001). *Bin Laden exploits technology to suit his needs*. CNN.com. Available: http://www.cnn.com/2001/US/09/20/inv.terrorist.search/ [2001, Sep 22].

Silver, B., & Slater, E. (1999). The Social Origins of World Hegemonies. In G. Arrighi & B. Silver (Eds.), *Chaos and Governance in the Modern World System* (pp. 151-216). Minneapolis: Univ. of Minnesota Press.

Silverman, D. (1993). *Interpreting Qualitative*. Thousand Oaks, CA: Sage.

Skocpol, T. (1977). Wallerstein's world capitalist system: a theoretical and historical critique. *American Journal of Sociology, 82*(5), 1075-1090.

Stallabrass, J. (1995). Empowering technology: the exploration of cyberspace. *New Left Review, 211*(3), 3-32.

Stephenson, W. D. (2002). Homeland security requires Internet-based thinking -- not just technology, [Webpage]. *Journal of Homeland Security*. Available: http://homelandsecurity.org/journal/Articles/Stephenson0102.htm [2002, Jan 22].

Sterling, B. (1993). *The Hacker Crackdown*. New York: Bantam Books.

Stinger. (Pseudonym). Chatroom interview, Jan 2002.

Stone, A. R. (1995). *The War of Desire and Technology at the Close of the Mechanical Age*. Cambridge, MA: The MIT Press.

Swartz, J. (2001). *Experts fear cyberspace could be terrorists next target: USA, world's most wired nation, has much to lose*. USA Today. Available: http://www. thehacktivist.com/article.php?sid=97&mode=thread&order=0 [2001, Oct 10].

Taylor, M. (1999). The dynamics of US managerialism and American Corporations. In D. Slater & P. J. Taylor (Eds.), *The American Century* (pp. 51-66). Malden, MA: Blackwell.

Taylor, P. J. (1981). Political Geography and the World-Economy. In A. D. Burnett (Ed.), *Political Studies from Spatial Perspectives* (pp. 157-172). New York: John Wiley & Sons Ltd.

Taylor, P. J. (1987). The Paradox of Geographical Scale in Marx's Politics. *Antipode, 19*(3), 287-306.

Taylor, P. J. (1991). The crisis of the movements: the enabling state as quisling. *Antipode*, *23*(2), 214-228.

Taylor, P. J. (1992). Tribulations of transition. *The Professional Geographer, 44*(1), 10-12.

Taylor, P. J. (1993). The last of the hegemons: British impasse, American impasse, world impasse. *Southeastern Geographer, 33*(1), 1-22.

Taylor, P. J. (1996). *The Way the Modern World Works: World Hegemony to World Impasse*. West Sussex: John Wiley & Sons Ltd.

Taylor, P. J. (1999). *Modernities: A Geohistorical Interpretation*. Minneapolis: University of Minnesota Press.

Taylor, P. J. (2000). A metageographical argument on modernities and social science. Unpublished manuscript, *Papers in Social Theory* (Special"Plurality of Modernities" Edition).

Taylor, P. J. (2001). Metageographical Moments: a Geohistorical Interpretation of Embedded Statism and Globalization. In B. Denemark & M.A. Tereault (Ed.), *Odysseys* (First Draft -- September 2000 ed.): Yearbook of International Political Economy.

Taylor, P. J., Beaverstock, J., & Smith, R. (2000). World-city network: a new metageography? *Annals of the Association of American Geographers, 90*(1), 123-134.

Taylor, P. J., & Flint, C. (2000). *Political Geography: World-economy, Nation-state, and Locality* (4th ed.). Essex: Prentice Hall.

Tetzlaff, D. (1998, Nov 6-7). *Yo-ho-ho and a server of warez: Internet software piracy and the new global information economy.* Conference paper: Magic, Metaphor, and Power: The WWW and Contemporary Cultural Theory, Drake University.

Vaida, B. (2001). *Cybersecurity chief pushes early-warning system*, [Webpage]. Government Executive Magazine. Available: http://www.govexec.com/news/ index.cfm?mode=report&articleid=21712 [2002, Jan 24].

Valeri, L. (2000). Securing Internet society: toward an international regime for information assurance. *Studies in Conflict and Terrorism*, *23*, 129-146.

Wallerstein, I. (1987). The United States and the World 'Crisis'. In T. Boswell & A. Bergesen (Eds.), *America's Changing Role in the World-system*. New York: Praeger.

*War Games*. (1983). MGM Studios.  Original Theatrical Release: June 3, 1983.

Ward, M. (2001, June 11). *Treaty 'could stifle online privacy'*, [Webpage]. BBC News. Available: http://news.bbc.co.uk/hi/english/sci/tech/newsid_1378000/ 1378482.stm [2001, Dec 17].

Ware, W. H. (1997). *The Cyber-Posture of the National Informatio Infrastructure*, [Webpage]. RAND. Available: http://www.rand.org/publications/MR/ MR976/mr976.html [2002, Jan 28]

Warf, B., & Grimes, J. (1997). Counterhegemonic discourses and the Internet. *The Geographical Review*, *87*(2), 259-274.

Wellman, B. (2001). Computer networks as social networks. *Science, 293*, 2031-2034.

Whine, M. (1999). Cyberspace -- a new medium for communication, command, and control by extremists. *Studies in Conflict and Terrorism, 22*, 231-245.

Wray, S. (1998a). *Electronic civil disobedience and the World Wide Web of hacktivism: a mapping of extraparliamentarian direct action net politics*. New York University Web Site. Available: http://www.nyu.edu/projects/wray/wwwhack.html [2000, Oct 16].

Wray, S. (1998b). *Towards bottom-up information warfare: theory and practice: version 1.0*. Electronic Civil Disobedience Web Site. Available: http://www.nyu.edu/ projects/wray/BottomUp.html [2000, Oct 13].

Wright, L. (2001, November). Keyboard one-on-one. *The Writer, 114,* 16-18.

Wriston, W. B. (1997). Bits, bytes, and diplomacy. *Foreign Affairs, 76*(5), 172-182.

Youngs, G. (1999). Virtual voices: real lives. In W. Harcourt (Ed.), *Women@Internet: Creating New Cultures in Cyberspace* (pp. 55-68). London: Zed Books Ltd.

Zakaria, F. (1998). *From Wealth to Power*. Princeton: Princeton University Press.

## Appendix A: Online Subject Implied Consent Form

### Informed Consent Form for Behavioral Research Study

| | | |
|---|---|---|
| **Title of Project:** | The Emerging Geopolitics of Cyberspace: Territorial Sovereignty and the Nodal Network | |
| **Persons in Charge:** | Ian Oas<br>Dept. of Geography<br>336 Walker Bldg.<br>Penn State University<br>University Park, PA 16802<br>ianoas@psu.edu | Professor Colin Flint<br>Dept. of Geography<br>302 Walker Bldg.<br>Penn State University<br>University Park, PA 16802<br>flint@geog.psu.edu |

**This section provides an explanation of the study in which you will be participating:**

a) The study in which you will be participating is part of a research project intended to gain information on varying spatial perspectives of cyber-conflict between individual agents (i.e., persons with access to technology) and U.S. Government agencies. The aims of this research are to explore differences between the traditionalist territorial perspective of the state and the perspectives of cyber-agents operating within the nodal network of the virtual world. The information from this study will hopefully contribute to the understanding of the globalization of politics being ushered in by the Internet and other telecommunications technologies.

b) If you agree to participate in this research, you will be asked to answer an in-depth questionnaire – via email or private messaging. In this questionnaire you will be asked questions about your spatial perceptions of the Internet, your personal political philosophy, reasons you use the Internet as an organization, hacktivist or hacker, rationale behind your online activism, and your opinion of the media's portrayal of hacktivists, online organizations, and/or hackers. The attached electronic questionnaire can be filled out at your convenience.

c) The length of time that you commit to answering the questionnaire is completely up to you. As regards an online interview via private messaging in a chatroom, estimated completion time is *no more than one half-hour*. We encourage you to take your time in responding in order that you might be able to think over your answers. Regarding responses via email questionnaires, you may take as long as you like – how much you write is completely up to you.

d) The study will involve the use of your written communication via the Internet. Your responses will remain completely anonymous once in my possession. Upon conclusion and return of the questionnaire, your comments will be retyped into a plain text file with a fake name. The original copies will be immediately deleted and destroyed. Though you will remain entirely anonymous, interception of your answers by third parties in cyberspace is a possibility. Also, though I will delete your answers on my Web-based email account, a chance exists that the account provider will maintain backup copies of the email.

e) In *no way whatsoever* is this study funded by, under the influence of, or in any way sympathetic to the United States Government, its allies, or any corporate entities. This is an independently funded study by a pauper graduate student interested in the geopolitics of cyberspace.

### This section describes your rights as a participant:

a) Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties. The investigator will make every effort to ensure that risk of third party interception is minimal, but total security on the Internet is impossible.

b) You may *ask any questions* about the research procedures *at any time*, and they will be answered.

c) Your participation is *voluntary*. You are *free to stop participating* in the research *at any time*. You *may also decline to answer any specific questions* as you see fit – without penalty.

d) This study involves minimal risk; that is, *you will not experience risks* to your physical or mental health beyond those encountered in the normal course of everyday life. The only possibility of disclosure of your answers is if my data is subpoenaed; though, even then, your anonymity will remain intact, as I will have no correlating online signatures to the response.

### This section indicates that you are giving your informed consent to participate in the research:

I agree to participate in a scientific investigation of hackers, hacktivists, and online organizations, as an authorized part of the education and research program of the Pennsylvania State University.

I am of 18 years of age or older.

I understand the information given to me, and I have received answers to any and all questions I have about the research procedure. I understand and agree to the conditions of this study as described.

To the best of my knowledge and belief, I have no physical or mental illness or difficulties that would increase the risk to me by participating in this study.

I understand that my participation in this research is voluntary, and that *I may withdraw from this study at any time* by notifying the person in charge.

I understand that I should print a copy of this consent form for my records.

By completing and returning the questionnaire/electronic interview to Mr. Oas, my consent to the above terms is implied.

Approved by the Pennsylvania State University Office of Regulatory Compliance, November 2001. http://www.research.psu.edu/orc/

## Appendix B: Example Questionnaire for Hackers

### Interview Questions for Online Subjects

1) What is your highest level of education (e.g., high school, some college, undergraduate degree, graduate degree, etc.)?

2) Do you consider yourself a politically active person? If so, how do you participate politically?

3) What are your primary political concerns when you use the computer or computer networks in a political capacity?

4) What purpose does using the computer as a tool serve for you, e.g., economic, protest, information dissemination, etc.? (Please note, “using the computer” is meant to be very broad, meaning anything from sending petitions, emailing Congressmen, or simply downloading programs, media files (mp3s), etc. It *does not* necessarily mean breaking into a computer system or anything of such overt nature. I don’t want details.)

5) Are you involved in activism in your local community? Do you consider yourself an active member of your community? If so, how?

6) Do you have a sense of purpose, mission, or long-term goal when you operate or spread data online? What is the scale of this “purpose”? (E.g., global, domestic/statewide, local, universally, et cetera.)

7) What is your stance on globalization? What is your view of free trade? Are you concerned by “globalization,” and if so, in what way?

8) Whom or what do you view as your primary adversary or adversaries in cyberspace? What are the causes of conflict with above stated adversary or adversaries? Are they real world adversaries (state governments, political parties, et cetera) or strictly virtual ones (hackers, online organizations, et cetera)?

9) What makes online political/cracking activity worthwhile? How do you perceive it as being better or less efficient than protesting in the real world?

10) How do you spatialize cyberspace – how do you vision it as a space? What is its geography in your mind? (E.g., a landscape, a territorial domain, a city, a network, etc.)

11) Do you see yourself as harboring certain advantages over government or corporate interests while operating in cyberspace that you might not have in the real world? (For example, anonymity, safe due to jurisdictional problems, etc.)

12) Is future government intervention and regulation of cyberspace a major concern to you, why/why not and how?

13) If corporate takeover and commercialization of cyberspace is an issue, why? How do you feel about the commercialization of the Internet? Are you against what the Internet has currently become in this regard?

Thank you for taking the time to fill out this survey. Please email me if you have any questions. When completed, please email me this form with your answers typed in as well (researchian@yahoo.com). Once again, thank you very much.

Sincerely,

Ian Oas

MS Geography student, Penn State University

336 Walker Building
Penn State University
University Park PA 16802
Tel: 814.234.5910
ianoas@psu.edu
researchian@yahoo.com