

(Submitted to *E&P A* and accepted pending revision.)

“The Spatial Dementia of US Geopolitics: the Internet and
Metageographic Tensions”

Abstract

The interaction of online political agency with territorial politics is evident in the many agents using the network geography of the Internet to circumvent institutions of United States hegemony. The United States is dependent upon the concept of territoriality to maintain both its power and stability throughout the capitalist world-system, but the Internet offers agents an ability to circumvent territorial sovereignty and geopolitical institutions of control. The US realizes that unimpeded, online agents threaten the force propelling the hegemony – the fluid and controlled exchange of high value information capital. However, it is argued that the US currently suffers from “spatial dementia” – its attempts to adapt to the security risks of the networked geography of cyberspace are undermined by territorial dependence and assumptions. Furthermore, it is hypothesized that due to the state’s dependence on territoriality, only a strategy of cooperation by the United States with the networked trans-national corporations controlling the cyber infrastructure will likely allow for stability in the virtual world. In turn, it is speculated that such a development may lead to the inevitable decline of US hegemony, and forge a new type of institution, a corporate ultra-hegemony, within a network metageography.

Keywords: Internet, hegemony, geopolitics, network metageography

Introduction

Cyber attacks against U.S. networks and infrastructures have increased dramatically in the past five years – from 3,734 registered attacks in 1998 to more than 82,000 attacks in 2002 (CERT, 2002). During the 1990s the United States moved a vast majority of its industry, business, services, and critical infrastructures into the networked geography of the Internet, with little regard for the potential security risks that would indubitably arise from such actions. Due to the fact that today nearly all critical infrastructures behind United States power are dependent on the Internet to function properly, the U.S. government has an interest in establishing regulations and protecting its political and economic institutions in cyberspace. However, attempting to catch-up in cyber-security is proving difficult for the United States, because online agencies are often deterritorialized and networked around the world. Furthermore, the United States suffers from *spatial dementia*: territorial strategies of power are so engrained in its institutional underpinnings that thus far it is incapable of modernizing its real world role into cyberspace.

Social movements and individual online agents utilizing cyberspace for political purposes comprise an important and researchable process in the deterritorialization of geopolitics at this point in history. This study will contribute to the growing amount of literature attempting to understand the deterritorialization of post-modern geopolitics as part of a broader, systemic process currently linked to U.S. hegemonic decline (Agnew and Corbridge, 1995; Flint, 2001a, 2001b; Taylor, 1993, 1996). Though numerous pieces of

literature discuss the deterritorialization of geopolitics and shed light on its various explanatory factors (Agnew, 1994, 1998, 1999; Agnew and Corbridge, 1995; Arrighi, 1994; Hudson, 2000; O'Tuathail, 1996, 1998a, 1998b, 2000; Taylor and Flint, 2000), relatively few have concentrated on the links between the geopolitics of cyberspace, social movements, and nation-states. This work will focus on the geographic tensions evident in the conflict between online dissidents and a U.S. hegemony attempting to regulate a networked, virtual space it helped create. Finally, heeding Flint's (2001a) call for attempting to place post-modern geopolitics into a historical materialist framework, this piece will use a geohistorical lens in its analysis of the deterritorialization of geopolitics (O'Tuathail, 2000), and therefore contribute to the potential accumulation of similar studies.

As the Internet continues its rapid expansion into households and institutions around the world online attacks have continued to increase. More importantly, the Internet has found itself of particular use for political purposes by a variety of actors (Chroust, 2000; Froehling, 1997; Ronfeldt, et al., 1998; Sieberg, 2001; Wray, 1998). Many online agents and resistances are aimed, either directly or unwittingly, at institutions of United States hegemony. This is to be expected, as the United States is entering a period of hegemonic decline (Agnew, 1993, Agnew 1998; Arrighi, 1994; Arrighi and Silver, 1999; Taylor, 1993, 1996, 1999; Taylor and Flint, 2000). During periods of hegemonic decline attacks on the hegemony become more common, more violent, and the hegemony's past ability to bring about political consensus around its ideological

underpinnings becomes fragmented (Arrighi and Silver, 1999; Taylor, 1996; Taylor and Flint, 2001). Many studies looking at hegemonic decline have concentrated upon inter-state competition with the hegemony, as in the past competition with the world hegemon was usually between states (Taylor, 1993).

However, hegemonic decline always brings with it a process of deterritorialization of politics (Arrighi, 1994; Flint, 2001a). Today's rapid deterritorialization of geopolitics is part of the larger process of the hegemonic cycle within the capitalist world-economy, and thus, it is predicted that geopolitics is likely to reterritorialize again (Arrighi, 1994; Agnew, 1993, 1998; Flint, 2001a; Flint, 2001b; O'Tuathail, 1998). On the other hand, some argue that US hegemonic decline differs from those of the past (Taylor, 1993, 1996). It is hypothesized that perhaps the world-system is on the cusp of a metageographic shift from a territorial based political geographic power structure to one based on networks and flows (Agnew, 1994, 1999; Taylor, 2000, 2001; Taylor and Beaverstock, 2000). It would be impossible for a state hegemony to function in such a world, and instead a new coalescence of power would have to rise in a network fashion, perhaps a linking of core agencies around the world in a type of "ultra-hegemony" (Taylor, 1996). By looking at online political agency, this paper will discuss the likelihood of these two outcomes.

Online dissidence as part of hegemonic process

Though proponents of continued U.S. world power exist (Hardt and Negri, 2000; Modelski, 1987), their calculations are frequently based upon a narrow set

of variables, primarily U.S. political and military capabilities. Often such calculations are undermined by episodic thinking and not placed in a broader temporal framework (Wallerstein, 1998). Studies based on geohistorical analysis and comparisons to past hegemonies overwhelmingly conclude that, though the United States remains strong both militarily and economically, it is in fact declining (Agnew, 1993, 1995; Arrighi, 1994; Arrighi and Silver, 1999; Taylor, 1993, 1996, 2000). Hegemonic power is not derived from military and political ability alone, but rather from three realms: economic dominance, political-military capability, and integrative power (Arrighi, 1994; Boulding, 1989; Taylor, 1996, 1999; Taylor & Flint, 2000). Furthermore, hegemony is best understood as a cyclical process within the capitalist world-system that historically lasts approximately 100 years – termed the hegemonic cycle – and forges a geopolitical order around its integrative power base.

Though hegemony in the capitalist world-system is defined as a state operating at the international scale, world-systems theory incorporates important elements of Gramsci's (1971) intra-state analysis of hegemony. Gramsci (1971) argues that the hegemonic power of the dominant class lies in its ability to build consensus and does not require force or violence to create an order in internal politics. Thus, when consensus is lacking and force is needed to induce control over rival classes, hegemonic order is either declining or no longer present. International systems theorists argue that the world hegemon functions in the same manner. International relations theorists have adapted Gramsci's theory to the inter-state level of analysis – where one state becomes dominant and forges

global cooperation through its consensus making abilities (Keohane, 1984). Boulding (1989) has called this integrative power. In contrast to destructive (e.g., violence) and productive powers (e.g., ideas, innovations, and technological developments), integrative power involves the ability to build organizations, create groups, inspire loyalty, and develop legitimacy, but also has the downside of creating enemies, alienating people, and thus in addition to its positive manifestations always maintains a shadowy self-destructive tension (Boulding, 1989: 24-25). World hegemons use integrative power to get states to willingly defer to the hegemony's desired order within the capitalist world-economy (Keohane, 1984). To use pure force to accomplish such international consensus would illustrate a lack of hegemonic authority and would be too expensive for a hegemonic power to maintain (Arendt, 1969; Keohane, 1984; Modelski, 1987).

The hegemony is the indisputable world leader in economics, rising to power through dominance of trade, production, and finance (Arrighi, 1994; Taylor, 1996; Taylor & Flint, 2000: 67). Much of the hegemony's power is derived from extrapolating more surplus capital from the world-economy than any other state institution (Arrighi, 1994; Taylor and Flint, 2000). Due to its economic position, the hegemony is always attempting to expand the capitalist world-system into new spaces in order to use its advantage to gain yet more surplus capital (Arrighi, 1994). Thus, the growth of global free trade and opening of new markets is paramount to the hegemony's ability to maintain global power and order, particularly as competition from other agencies begins

to grow. Free trade is needed in order for surplus capital to continue flowing to the hegemonic state. The fewer barriers to fluid trade the better for the United States. However, some societies will attempt to thwart the flow of free trade to protect their domestic markets (Escobar, 2001).

There are several ways for the hegemony to contend with such dissension, the most obvious method being through the threat of its dominant military force (Modelski, 1987; Waltz, 1979). Yet, the hegemony at the height of its 100-year cycle rarely needs to use military force – as was evident for the U.S. following the Second World. In contrast, the Korean conflict represented a beginning warning sign for the US that its hegemonic height was over – culminating a decade later in the quagmire of Vietnam. Before decline, merely the threat of force, or severe economic sanction, is generally enough to pull all but the largest competitors of the world-economy in line (Agnew, 1993, 1998; O’Tuathail, 1996). For those that are initially obstinate to the hegemony, the hegemony can offer economic enticements to prompt obedience. From the eventual global acquiescence forged during the height of the hegemonic cycle, a geopolitical order (Agnew, 1998; Keohane, 1984) is formed around the ideologies of the hegemony.

But there is much more to hegemony than simple economic and military superiority. Two oft glossed over aspects of hegemonic analysis are extra-territoriality and prime modernity. Extra-territoriality is the process by which the hegemony spreads its political and economic sovereignty over other states’ territory in order to better exploit them (Hudson, 2000). By setting up

international institutions (i.e., UN, NATO, IMF, etc.) the hegemony is able to expand its power into other territorially bound institutions without conceding its own sovereignty (Arrighi, 1994; Hudson, 2000; Taylor, 1996; Escobar, 2001). The creation of such institutions allows U.S. interests and political ideologies to have direct input and guidance on particular political and economic decisions of other sovereigns and localities (Escobar, 2001). This helps keep markets open from interference of capital exchange and maintains a stable geopolitical order in which capitalist processes can operate smoothly (Arrighi, 1994; Keohane, 1984; Taylor, 1996; Taylor and Flint, 2000).

However, the hegemony also maintains an empowering social method for infiltrating other sovereignties as well – the prime modernity (Taylor, 1999). Taylor (1999) defines “prime modernity” as being synonymous with the hegemony itself, as its technological prowess and society come to be viewed around the world as the epitome of modern – the hegemony becomes what most societies want to emulate. Prime modernity is an instrumental tool used by the hegemony to ideologically export “a way of life” (Flint, 2001a, 2001c; Taylor, 1999). Of course, the prime modernity is often centered on aspects of economic innovation and lifestyle. Thus, under Dutch hegemony mercantilism, and with the British industrialization, were the prime modernities (Taylor, 1996, 1999). The United States’ prime modernity is focused on mass-consumerism. Rather than remain a benign element of others’ envy, however, by universalizing its modernity as the path to the future, the hegemony cajoles other societies into

opening their economies to the capitalist world-system and into believing that emulation will a modern society make.

Unfortunately, the prime modernity is a fallacy, an impossible goal for most societies of the world (Taylor, 1996, 1999). Due to the dominant position the hegemony maintains in gaining surplus capital through the core-peripheral processes of capitalist exchange, those aspiring to the prime modernity are at a severe disadvantage (Arrighi and Silver, 1999; Taylor, 1993, 1996, 1999).

Some societies come close to acquiring a similar modernity status, but a vast majority will never achieve the “American Dream.” Hence, it is only a matter of time before those peripheralized by the capitalist world-system begin to focus political action against the futile promises of prime modernity, often while proposing alternative methods of social organization (Flint, 2001c; O’Tuathail, 1998).

Those opposing various aspects of U.S. prime modernity have been provided a new means through which to contest and confront hegemony – using the non-territorial geography of cyberspace as a space of resistance (Castells, 2000; Himanen et al., 2002; Lenk, 1997; Pile, 1997). Through the technological innovation of the Internet, developed under U.S. hegemony and used as yet another method of extra-territoriality, a new social geography has been created (Castells, 2000; Himanen et al., 2001; Mitchell, 1999; Poster, 1995; Rheingold, 2000; Ross, 1991; Wellman, 2001), providing groups and individuals interconnected around the globe the ability to affiliate and act together. The Internet provides a geography in which persons can reorganize and mobilize

around non-territorially defined issues and through which they can subvert traditional institutions of power that are based on concepts of territorial sovereignty (Castells, 2000; Everard, 2000; Himanen et al., 2001; Luke, 1998; Rosecrance, 1996; Ross, 1991; Wellman, 2001; Wray, 1998a, 1998b; Wriston, 1997; Youngs, 1999). Though other means and forms of deterritorialized politics currently flourish, agents operating in cyberspace present one of the most threatening forms of resistance to U.S. hegemonic power (PCIPB, 2002). For the non-contained agents of cyberspace operate freely in the same network geography in which the most valuable capital underlying hegemonic surplus accumulation is located – information, knowledge, and finance.

Despite the importance of cyberspace, the United States is also dependent upon the concept of territoriality to maintain both its hegemonic power and stability throughout the capitalist world-system. It relies on its own territorial sovereignty to protect its political and economic interests, and as already mentioned, uses prime modernity and extra-territoriality to infiltrate and spread its sovereignty over other states. Silver and Slater (1999) argue that the process of expanding extra-territoriality actually plays a dynamic role in a hegemon's eventual decline. In its ascension to power, the hegemony makes a social compact with anti-systemic movements and agents (Silver and Slater, 1999) – offering them the prime modernity and the right to exist if they participate in the new order. Over time, however, these promises fail to be met, and in turn, the social compact fragments and order begins to fray (Silver and Slater, 1999). As the traditionally infallible concept of territorial demarcation

and control is called into question by the extent of hegemonic extra-territorial power held over other state institutions, geopolitics begin to deterritorialize. The hegemony's role as a container of surplus capital and dominant core processes is challenged. Thus, territoriality serves a crucial role as the container of dominant core processes and surplus capital accumulation on which power in the world-economy is based. Without the concept of territorial based political institutions, hegemony is not possible; in fact, many argue the capitalist world-system would cease to exist (Arrighi, 1994; Taylor, 1993, 1996; Taylor and Flint, 2000; Arrighi and Silver, 1999). Thus as the dominant institution in, and protector of, the capitalist world-economy, from the U.S. perspective it is imperative that it maintain the function of territorial sovereignty in the geopolitical order. Yet, paradoxically, it must also attempt to continually build its power on concepts of extra-territoriality that thwart the relevance of sovereignty in the inter-state system.

Thus far the United States has been impotent to stymie anti-hegemonic agents operating in the extra-territorial virtual space it created. The U.S. is suffering from spatial dementia – territorial organization and strategy are so engrained within its mechanisms and functions of power that it has thus far been incapable of adapting to non-territorial adversaries. In essence, the spread of the capitalist world-economy into the network geography of cyberspace has presented incalculable new risks to the U.S. hegemony's position of power, manifesting in the ability of anti-hegemonic, non-state agents to operate with impunity, regardless of U.S. extra-territorial abilities, and attack the United

States in spaces from which it derives its power. Hegemonic transition or a systemic crisis is liable to result unless the United States comes to deal with the risk of deterritorialized agents operating in cyberspace against its prime modernity.

Online Agents and Contemporary Deterritorialized Geopolitics

As the world hegemony has difficulty in adapting to the new geographic risk it has invented, political agents utilizing cyberspace in various capacities have begun to proliferate and grow in strength. Meanwhile, the network geography of the virtual world continues to spread without overarching authority (Loader, 1997: 4). As this happens, movements concerned with various political issues have begun to identify themselves, as well as inform, connect, organize, and mobilize new individuals, around various social issues in a deterritorialized landscape that has no borders (Brunn, 1999).

In cyberspace deterritorialized political agency intersects with the territorial politics of the real world. In opposite fashion to the complications faced by state actors with territorially defined spheres of influence, however, non-state agents in cyberspace enjoy the advantage of fluid movement, communication, and network structuring – they are mobile and diffuse, not cemented in the real world. Furthermore, networked agents operating in cyberspace are confident, realize the advantages that the geography of cyberspace provides them, and rather than adapting to the geography of the network, are often in the critical position of being able to continually reinvent

and shape this networked space to keep it beyond the control of traditional political actors.

During 2002, 10 interviews were conducted with hackers in order to gain insight into their spatial and political perspectives of online conflict with real world political institutions. The participants of this study, their names changed herein to ensure anonymity, were selected due to their willingness to participate in a lengthy interview and subject themselves to follow up questioning. All of the respondents spent a considerable amount of time, often more than once, answering my questions in various online hacker chatrooms. Though small in number, the information provided from the interview subjects lends accurate credence to the problem statement outlined at the beginning of this paper that within online resistances against the US hegemony a shift to a network metageography is manifest.

The methodological approach used in this study was that of the exploratory case study, which is meant to focus on a particular issue, illuminated by a limited number of cases (Creswell, 1998: 62). The issue in this study is the extension of individual political agency into the nodal network of the Internet and its role in confronting U.S. hegemonic power and interests. This study uses a “holistic analysis” (Creswell, 1998: 63) of all the coded interviews to better illustrate the impact of online political agency in the geopolitical world order. In general, case studies maintain a limited amount of samples, or cases, so as to not water down the research (Creswell, 1998). Intense analysis of a few samples is often preferred over a large quantity of

samples (Creswell, 1998). Though it must be noted that this sample is not definitively thorough – as there are millions of online agencies around the world – from these interviews particular themes relevant to the hypothesis were successfully extracted.

For simplification in this study, hacking and cracking¹ are combined under the umbrella term “hacking,” which in turn is defined as using information and communication networks to partake in actions that would be impossible to successfully do in the real world. Often this means breaking into secure networks, reprogramming others’ space, or stealing information capital, but it can also mean incidentally infiltrating spaces that one would not be able to visit in the real world. Today’s Internet was primarily invented, developed, and formed by hackers – people experimenting out of curiosity and continually pushing the envelope on new network technologies (Hactivist.com, 2001; Himanen et al., 2001). However, over the last twenty years, the U.S. hegemony and global society have come to depend on interconnected information networks for a plethora of critical infrastructural needs, those with the potential to navigate and reorganize these networks increasingly find themselves vilified and stereotyped by institutions whose powers are threatened by their existence.

Much of society’s view on the risk of hacking stems from actual, though quite irregular, hacker attacks on the United States and its infrastructures during

¹ The difference in definition between “hacking” and “cracking” is contestable. However, hackers are generally considered people who are programmers and good at computer innovations, whereas crackers are more malevolent, purposefully using their programming and network skills to break into secured computer-network systems.

the late 1980s and 1990s (Freedman & Mann, 1997; Hafner & Markoff, 1995; Sterling, 1993). In general, hackers with a political agenda have often targeted the United States government, its allies, or corporate agencies attached to the Internet as a form of protest or for pure opportunism. These virtual “break ins” on state powers are not synonymous with traditional conceptions of “invasion” or “illegal immigration.” In fact, numerous electronic intrusions in the United States come from people residing within the world hegemon’s territorial sovereign. Once connected, place in the real world is of minimal consequence to agents operating online (Everard, 2000; Himanen et al., 2001).

Though hacker attacks often appear random and lack systematic function, they are inherently political. Though reasons for hacking vary drastically, the philosophies behind hacking have dire implications for the state of the capitalist world-economy. Though in most cases hacking stems from curiosity (Himanen et al., 2001), or as some hackers have noted “looking to have fun” (Darklaser) and “for pleasure, [with] no malicious intent involved” (K-Pax), the impact of their actions is extremely threatening to established institutions. Hacker agency is driven by gaining, and then figuring out how to maintain, access and interconnectivity to forbidden networks, the same networks on which accumulation in the capitalist world-economy is coming to depend, the result is a direct confrontation between the traditional protector of free trade, the U.S. hegemony, and individual hackers. Thus, the seemingly benign “curiosity” (Darklaser; K-Pax; Stinger) and “challenge” (Stinger) fueling hackers harboring no direct political philosophy becomes, nevertheless, very

political. The reasons why individuals hack matter not to the hegemony; what matters is the fact that hackers can operate without restriction. The following quote summarizes this well:

“I normally hack for the challenge of it. ... I don't really have any longer term goal, I just do it for fun. It's not really cool to mess up peoples' comp[uters] unless you have a good reason” (Stinger).

The fact that Stinger could “mess up peoples' comp[uters]” without displaying any fear of retaliation or discipline, therein lies the risk to U.S. hegemony.

Yet, thus far, attacks have not been overly precarious to national security or free trade. When asked about this, K-Pax notes that “Internet terrorists are really nonexistent because it takes too much effort to hack.” Though K-Pax views hacking “as a wonderful tool,” as concerns political uses he is more cautious, noting that it is definitely of use to political agents but “every tool has two uses, good and bad.” Definition of what is good use, as compared to bad use, however, is open to debate.

For quite contrary to being anti-capitalism, it is ironic that hackers threaten the hegemony perhaps more due to their unfaltering ethos of “free trade.” Certainly it would seem contradictory that hackers espousing that they “love capitalism ... as long as the big corporations don't screw everything up” (Phantom) and “have nothing against Microsoft ... [unless] they eliminate competition” (Stinger) could possibly pose a threat to U.S. hegemonic interests. For certainly they have wholeheartedly consumed the prime modernity of mass consumerism and neo-liberalism. However, hackers daily partake in a system of literal free trade – property once acquired is reproduced and given away for

free on the networks under the assumption that product diffusion and replication is a good thing for the masses. Thus, though in fact all of the hackers interviewed held the belief that “free trade is cool” (Lightblader), they often fail to acknowledge the fact that their style of product diffusion goes against the very processes upon which hegemony depends – surplus capital accumulation. The United States realizes that unimpeded, hackers and other online agents threaten the vitality of the force driving the capitalist world-economy, and propelling the hegemony, when they partake in information capital diffusion. Thus, regardless of whether online agents realize it, they represent a threat to institutions of power dependent upon capital accumulation.

Even though hackers understand that information and knowledge comprise valuable capital, their underlying ambition – to acquire and diffuse knowledge to the masses to promote equal access across all spaces (Freedman, 1997; Hactivist.com, 2001; Himanen et al., 2001; Ross, 1991; Sterling, 1993) – goes directly against the core-peripheral processes underlying the capitalist world-economy. A hacker’s view of the benefits from free trade differ radically from those of most economists: “It’s ironic but I normally [take] from companies that I really like ... cause I really like their programs ... [and] I don’t have thousands to blow on their software” (Phantom). Rather than seeing themselves as thieves or terrorists, many hackers feel like post-modern Robin Hoods, fighting against the unequal distribution of information and knowledge capital. Their motives are not directly concerned with changing the capitalist system, just distributing high value information and knowledge to the masses.

Practically echoing the cliché of any business school, Stinger notes that “in cyberspace knowledge is power while in the physical world money and goods [might] be more important,” and thus “the more knowledge you have the more power and sometimes [the] consequences [that] come with it.” Having the power to free and disperse this valuable knowledge is the risk hackers present to the hegemony, and this ethos is universal throughout the hacker community (Himanen et. al, 2001):

“Yeah... that’s the other thing, the democratization of information as opposed to monopoly by colleges and stuff. The idea that colleges have the correct information, that they’re the only ones authorized to distribute information. They had a lock on education before the net ... you couldn’t get access to that info unless you ... attended the colleges, which you could only do if you were rich. So in a sense the distribution of information is more democratic now or rather more socialist” (Darklaser).

K-Pax concurs, noting that “the internet is the greatest source of knowledge the world has ever known” and that traditional capitalist “regulations are almost impossible” there.

Online agents are not prone to believing that governments and corporations are going to sit by idly while this free trading goes on. However, due to their intrinsic position in creating and rerouting this networked geography, they are not fearful of government attempts at regulation. Though reasons varied, there was near 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 United States would attempt to even partake in such a colossal endeavor:

“I don’t really think we have to worry about government regulation of the Internet.” (Stinger).

For Stinger it comes down to a simple matter of economics – the costs of regulating the Internet far outweigh the potential gains in his mind “and they still couldn’t have it all regulated.” He believes that in the anarchy of cyberspace, the best a government can hope to do is to “regulate ... their servers” (Stinger).

Stinger’s mention of the cost aspect and the impossibility of one government ever regulating all of cyberspace raises some interesting points. For though the U.S. most certainly desires to maintain stability throughout the world-economy to facilitate the most fluid accumulation of capital possible, at this point in the hegemonic cycle it may not have the capital resources or the international cooperation to do so. Furthermore, it is likely impossible for a single state to govern the Internet. Probably only a strategy of cooperation by the United States with other networked powers can result in a comprehensive regulatory system.

Subconsciously, hackers are aware that the roots of their advantage in cyberspace are based in geography even if they are not versed enough in the spatial discipline to say so directly. K-Pax notes that, as concerns United States regulation, there are “too many inlets. The internet is based off ... the network structure. It breaks down a lot of barriers that our government tried to keep up.” Darklaser cuts straight to the crux of territoriality: “Well the thing is... which government? A state government can only regulate the server[s] in its country.”

Furthermore, Darklaser raises the question of defining responsibility in networked cyberspace:

“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?”

Darklaser does not believe that such problems make all regulation impossible, but he argues that the spatiality of regulation will need to change to be successful. Instead of governing by area, as traditional geopolitical institutions are inherently biased toward, regulation will only be possible directionally: “you can stop people from coming in (or at least try to) but how do you stop people from going out to a foreign server?” Unless the hegemony is capable of changing to this new geography, even regulation of direction will remain up to sub-state actors in control of the networks (e.g., corporations and hackers).

Hackers are not blind to the fact that the United States has already begun attempting to regulate the Internet. However, they argue that the U.S. will meet little success in achieving this goal, just as they have failed in regulating current network processes in the real world:

“I think they tried [regulating the Internet] and gave up. It’s as impossible as in the real world. They can’t stop illegal immigration either. People who want to come in will find a way” (Darklaser).

“Of course [the U.S.] will try to [regulate], they need their tentacles in everything. I don’t think they will be able to. The internet is anarchy.” (K-Pax).

Hackers also appear cognizant of the fact that lack of territorial affiliation also plays a key role in their abilities to avert particular everyday laws that function in the real world. When asked about the reasons behind their

powerful abilities and the failures of regulation in the virtual world, a plethora of spatial commentary follows. As Stinger espouses, "... the scale and complexity of the net 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 an untamable "virtual reality with connections to this reality." The Net's ability to circumvent real world borders is definitely "part of" the hegemony's problem.

Furthermore, the digitization of agency in cyberspace leads to problems of tangibility and identification, as "cyberspace is sort of a different world" connected to the real world that "deals strictly with information instead of solid objects," including human beings.

The anonymity of the Internet primarily comes from its network geography. By allowing human agency to interact in the digital landscape, cyberspace can be used as an appendage to real world human agency without threat of bodily harm. In essence, the state's legitimacy to use violence is meaningless in a digital landscape. Even when capable of defending particular nodes in the network, it is extremely difficult to discover an enemy's real world position – "it [is] an advantage to not be seen or recognized" (Stinger). Though many of those interviewed argue that "there is really no anonymity on the net," the fact remains that the success of states in identifying skilled online agents is remarkably low. The intangible geography of cyberspace allows individuals to partake in processes that would be impeded in the real world by established political institutions.

Established territorial methods of deterrence fail in network geographies. The scale of operations that deterritorialized groups of actors can achieve when globally organizing online easily overreaches the sovereignty of the territorial state, and thus common state methods of deterrence, such as the right to use violence, are compromised as a tool of control. 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. Harboring the most direct nodal links to 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 are not affiliated with any territorial entity.

U.S. Attempts at Adaptation to Network Conflict

Not surprisingly, analysis of policy documents published by the RAND² and ANSER³ Corporations, as well as several affiliate institutes, demonstrate that

² The RAND Corporation is a government-funded corporation specializing in informing U.S. government policy in strategic and military studies. Its corporate mission – to “promote scientific, educational, and charitable purposes, all for the public welfare and security of the United States of America” (Anonymous, 2002f) makes it one of the top publishers on U.S. defense strategy. RAND also works on the development of “theories and tools for decision-making under uncertainty,” contributing to the development of network theory (Anonymous, 2002f).

³ One of the major priorities of the ANSER Corporation (Advancing National Strategies and Expected Results) is to inform U.S. policy and strategy for homeland defense. Thus, ANSER operates the Institute of Homeland Defense. ANSER’s mission statement is to “help our nation’s public institutions cope with current and emerging challenges...” – Dr. Ruth David,

the United States has been attempting to modernize to Internet security risks for years. However, of more importance than the fact that the United States is cognizant of the “cyber-threat,” is how the U.S. is attempting to adapt to it. Analysis of documents demonstrates that though the United States concedes that the network geography of cyberspace puts them at a distinct disadvantage, they are primarily incapable of changing their strategies and methods of security to adapt to the new, deterritorialized risks – the result of spatial dementia.

The threat of information warfare has procured numerous antidotal competing policy recommendations (Anonymous, 1997; Buchan, 1996; Cilluffo, 2000; Ware, 1997). Though analysis of contemporary policy doctrines are split into two topics of discussion, those 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) and those focusing on asymmetrical attacks from non-state agents (Anonymous, 2001; Arquilla and Ronfeldt, 1999a, 1999c, 2001a, 2001b, 2001c; De Borchgrave et al., 2000; Fisher, 2001; Ronfeldt et al., 1998), one thing links all policy documents – an urgent and inherent call for drastic modernization of state defenses against digital network weaknesses.

CEO (Anonymous, 1999). It publishes the *Journal of Homeland Security*, in addition to producing a weekly newsletter with links to breaking stories and policies on homeland security and new warfare – with over 10,000 subscribers.

The Center for Strategic International Studies⁴ warns straight away that the information age “empower[s] individuals and non-state actors” around the globe (Cilluffo et al., 2000: 1). Larsen and David (2000) have added an important qualifier to this fact – non-state agents may “perceive justifiable reason to challenge America’s leadership” through the information networks. Whereas “protection of core values or vital interests within a sovereign space is one of the more universally accepted premises of national security,” today “the applications and processes [networked telecommunications] have engendered, do not succumb to territorial and geographical restraints” because “cyberspace ‘unbundles territory’” (Fisher, 2001). As Arquilla and Ronfeldt (1999b, 1999c, 2001a, 2001b) note in their cyber-security books, the most precarious attribute of any information war policy is that it may be based on false assumptions that do not pertain to networked conflict.

Review of U.S. policy and government documents illustrates that the advantage for anti-hegemonic online agents lies in the fact that they better understand the geography of conflict in cyberspace. Though policy informers such as Arquilla, Ronfeldt, and Fisher espouse the importance of fighting networks with networks and of the lack of territoriality in cyberspace, the U.S. as a state institution is incapable of promptly adapting to the new non-territorial threats. Furthermore, it often suffers from territorial assumptions at numerous

⁴ The Center for Strategic and International Studies is a private, nonpartisan, and tax-exempt institute comprised of 190 researchers addressing numerous realms dealing with policy and strategy – including the study of challenges to U.S. and international security.

levels of policy making (Anderson, 1999; Anonymous, 1997; Anonymous, 2001; Arquilla and Ronfeldt, 1996, 1999b; Buchan, 1996; Cilluffo et al., 2000; de Borchgrave et al., 2000; Dorobek, 2001; Gray, 1999; Molander et al., 1996; Mulvenon, 1999; Ronfeldt et al, 1998). For example, though it suffers over 20,000 network intrusions a year, rather than plan for attacks by non-state actors the Pentagon has largely concerned itself with defending against cyber-warfare from other states, still tainted with state-centric thinking when it comes to conflict (Fisher, 2001). In the *Journal of Homeland Security*, Larsen and David (2000) argue that “[a]n integrated warning/information ... system is required to ... mitigate effects during and after large-scale attacks and campaigns.” Such a hypothesis exemplifies the assumption that U.S. interests will be attacked by another state (Mulvenon, 1999; Vaida, 2001). The effectiveness such a system would have at identifying an attack against one particular node is likely minimal. Moreover, the idea of creating 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.

The binary between domestic and international (Agnew, 1994, 1998) defense contaminates the designation of separate cyber-security tasks to government defense institutions. Perhaps nowhere do these territorial conundrums come to light as glaringly as in the security and jurisdictional discrepancies lying between the Department of Justice and the Department of Defense. As the Pentagon suffers an increasing number of electronic intrusions

every year, 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 networked to the Internet, it finds itself with little or no jurisdiction to pursue attackers when it determines that an attack was initiated from overseas – for that is an international matter (Anonymous, 1998, p. 3-8). The recent establishment of a Department of Homeland Security does little to remedy the spatial enigma confronting the hegemony. In fact, cyberspace does not affect a “homeland” per se, but rather millions of separate nodes lying therein. Cyberspace not only fails to break down into domestic and foreign spheres, a majority of adversarial agents operating on the Net are rarely connected to, or affiliated, with any territorially based organizations.

Thus, it is here in these dichotomies between policy and sound strategy that the spatial dementia of the United States stands out. Adaptation to cyber-threats requires a thorough rethinking of strategy in a manner counter-intuitive to the geographic norms of the state. For such changes to occur on a massive scale and across all political institutions within the United States hegemony, mistakes and setbacks in policy will certainly be made. In fact, some have begun to argue that many of the policies initially instigated for cyber-defense were based on false spatial presumptions (Anonymous, 1998).

Even policy papers arguing that old security strategies need to be jettisoned for new ones are tainted with territorial assumptions that undermine their overall usefulness. One RAND report concluded that “key national military strategy assumptions are obsolescent and inadequate for confronting the

threat of I[nformation] W[ar]” (Molander et al., 1996: xvii), but then went on to continually refer to the “vulnerability of [the] U.S. homeland” to cyber-attack – displaying an inherent territorial bias in its envisioning of cyberspace. Both institutional and corporate hegemonic interests are under threat wherever they are around the world, not merely in the “homeland.”

A Networked Alliance: Corporate Cooperation

Perhaps a more realistic approach to security 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). As Stephenson (2002) notes in the *Journal of Homeland Security*, “with most American communications infrastructure owned by the private sector, partnership is a necessity.” 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 telecommunications companies will become “key player[s]” in the effort to secure information in cyberspace.

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 (Agnew, 1994; Taylor, 2001, p. 3). Metageography is a term “to describe the geographical structures through which people order their knowledge of the world” (Taylor, 2001, p. 3), a 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). The most recent technological feat of the U.S. hegemonic cycle, networked virtual space, is not only a tool facilitating capital accumulation but may be leading to “the deconstruction of national financial and cultural boundaries which are an intrinsic attribute of [the modern world-system]” (Loader, 1997, p. 9).

If a metageographic shift is being facilitated by the network geography of the Internet and the new geographies of socialization that the cyber structure facilitates, then the state institution will need to evolve or it may decline in relevance and power within the world-economy (Everard, 2000). The hegemony, of course, would need to lead other states in this modernization.

Yet, due to the inherent territorial underpinnings of the state institution, the only option for operating within a networked world may be to align the state with networked, trans-national corporations controlling the resources of the cyber infrastructure and capital. Through such an alliance, the state would have a networked ally to fight deterritorialized threats.

Under the Bush Administration, the newly formed President's Critical Infrastructure Protection Board (PCIPB) recently made partnering with corporations official U.S. policy (PCIPB, 2002). The inability of the United States government to secure cyberspace stems beyond the Net's lack of territoriality alone, but also centers on the fact that trans-national corporations have far more power in cyberspace than the United States, as they own the critical infrastructures, create the software used, and are already established in a network fashion (PCIPB, 2002). The "applications and processes ... engendered [by corporations], do not succumb to territorial and geographical restraints" (Fisher, 2001), and therefore, it has been successfully argued that an equal alliance between the U.S. government and corporations would be beneficial to the world hegemony (PCIPB, 2002). As the CSIS notes in their comprehensive report on cyber-threats, "[state s]ecurity is now the responsibility of each company, government entity and private institution" (de Borchgrave et al., 2000: iii). Much policy concurs with this analysis arguing that, through genuine cooperation between Federal agencies and private industry, the U.S. might forge a strategic alliance networked around the globe to help prevent attacks on U.S. interests (Anonymous, 1998; Cilluffo, 2000;

Molander et al., 1996). In fact, the PCIPB notes as part of its official statement of policy that it encourages the private sector to “develop plans to secure their parts of cyberspace” (2002: 8). The former Director of the National Infrastructure Protection Center concurs with this strategy, arguing that “security is not something ... the Federal government can do alone” (Vatis as quoted by Anonymous, 1998: 8). This represents a dramatic change in the policy of the US hegemony and perhaps for the state system in general; for, to delegate certain aspects of state security to the private sector may represent the beginning of a serious change in the role that the state will play within the capitalist world-economy (Everard, 2000).

Surprisingly, the amiable relinquishment of network security duties to the private sector may come quite easily from the various Federal agencies involved in such an historic handoff due to their own inability to adapt. Currently there is consensus in nearly all sectors of the U.S. government that contemporary strategy and policy for defense in cyberspace has been practically worthless (Cilluffo, 2000; Cilluffo et al., 2000; Fisher, 2001; Frank, 2001a, 2001b). It is plagued by contradictory policies, agencies, and assumptions based on territoriality. Furthermore, over 85% of the Internet network is not under government control but owned and operated by the private sector (PCIPB, 2002: 8). Furthermore, very few suggestions for modernizing government institutions to these issues are capable of throwing off the yoke of territorial strategies and assumptions that the state depends upon. The dichotomy between theoretically discussing networks in policy and implementing necessary changes

in territorially based federal institutions has led to a hegemonic headache (Fisher, 2001; Larson and David, 2000).

Conclusion

As this case demonstrates, the United States hegemony is engaged in a conflict with various political agents using the Internet as a geography of resistance. Furthermore, as a territorially based political institution, the United States is having difficulty adapting to the threats that the new network geography of global resistance provides. It has been argued that the rise of online network agents confronting U.S. hegemony is part of the larger process of hegemonic decline. Deterritorialized threats of all types symbolize this, but the surge in online agency provides a most explicit example of the world hegemon losing its ability to forge geopolitical stability through traditional means of control and regulation. Try as it might, the only way to fight networks is with networks (Arquilla and Ronfeldt, 1996, 1999a, 1999b, 1999c, 2001a, 2001b), and traditional territorially based strategies and methods will not work for the United States hegemony in confronting networked agents. Unless the United States awakes from its current spell of spatial dementia, online resistances will maintain a distinct advantage (Arquilla and Ronfeldt, 1996, 1999a, 1999b, 1999c, 2001a, 2001b) – continuing to expand and grow, as well as shape the geography of the conflict.

Though this piece does not proffer evidence for prediction, some speculative outcomes do arise. Failure to adapt to deterritorialized threats may result in Taylor's (1993) "last of the hegemons" hypothesis – where the U.S.

declines as hegemon and no territorial state is capable of gaining the economic and cultural power needed to become hegemony. A metageographic shift may also be the outcome – if people begin to deterritorialize their identities and organize in communication networks to the point of changing the role of the nation-state (Everard, 2000; Taylor, 2001).

Theories of systemic change aside, perhaps the United States will simply proceed down the path of other hegemonies. Geohistorical analysis illustrates that during past hegemonic declines power sharing and cooperation between the hegemony and other core powers has occurred to ensure the seas stay open for the continuation of trade and the stability of the capitalist world-economy (Arrighi, 1994; Arrighi and Silver, 1999; Keohane, 1984). Traditionally these other powers are core powers that also have an economic interest in helping the hegemony maintain the capitalist world-economy. Today it appears a parallel happenstance may be occurring with the U.S. aligning with trans-national corporations (Arrighi, 1994; Taylor, 1993; Taylor, 1996; Taylor and Flint, 2000). Though the medium through which capital is exchanged is different today – from shipping goods via the sea to packeting information across the fiber optic virtual world – it is of crucial importance to the hegemony that the Internet remain secure for capitalism, so that maximum profitability can be gained from networked commerce. Arrighi and Silver (1999) argue that one of the driving impetuses behind declining hegemonies making such alliances with regional powers is cost. As the U.S. has made it official policy to call upon corporations to help secure online commerce, finance, and trade from “online

terrorists” (PCIPB, 2002), certain parallels between past hegemonic declines and the U.S. become evident.

Though an alliance with a corporation is different from an alliance with another state, such a move should not be completely unexpected. Taylor (1993) argues that it is impossible for another state hegemony to rise, and instead an “ultra-hegemony” may form from the cooperation of core agencies around the world – i.e., core corporate and bureaucratic processes united through a world city network (Taylor, 1996). Such a monumental conclusion is certainly not possible from the case here, but hopefully further evidence may be cumulated to either give credence to or falsify such a hypothesis. What is certain is that cyberspace has ushered in a dynamic new geography for resistance against the world hegemony, a geography that necessitates adaptation on the part of the United States, and that has induced a type of spatial dementia in regards to strategies and philosophies of national security and homeland defense, as being the hegemony of a territorial metageography hinders adaptation to networked threats.

Acknowledgements

I would like to thank my advisor, Colin Flint, for his great mentoring and help. Also, special thanks must go to Birgit Ulrika Mühlenhaus and Heiko Fürst for their comments and support.

References

- Agnew J, 1993, "The United States and American Hegemony", in *Political Geography of the Twentieth Century: A Global Analysis*, Ed. P J Taylor, New York, Halsted Press, pp 207-238
- 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*, 28, 3 pp 499-521
- Agnew J and Corbridge S, 1995, *Mastering Space: Hegemony, Territory and International Political Economy*, New York, Routledge
- Anderson R H, 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*, National Defense Panel, Website, Jan 23, <http://www.fas.org/man/docs/ndp/front.htm>
- Anonymous, 1998, *Seminar on Cyber-Terrorism and Information Warfare: Threats and Responses: Proceedings Report*, Potomac Institute for Policy Studies, Online PDF, Jan 22, <http://www.potomac institute.com/pubs/cyber.pdf>

- Anonymous, 2001, *Information Assurance and Critical Infrastructure Protection: A Federal Perspective (White Paper)*, GEIA, Online PDF, Jan 19
- Arendt H, 1970, *On Violence*, New York, Harcourt, Brace & World
- Arquilla J and Ronfeldt D, 1996, *The Advent of Netwar*, Santa Monica, CA, RAND
- Arquilla J and Ronfeldt D, 1999, "The Advent of Netwar", *Studies in Conflict and Terrorism* **22** pp 193-206
- Arquilla J and Ronfeldt D, 1999, *The Emergence of Noopolitik: Toward an American Information Strategy*, Santa Monica, CA, RAND
- Arquilla J and Ronfeldt D, 1999, "Networks, Netwar, and Information-Age Terrorism", in *Countering the New Terrorism*, Ed. I O Lesser, B Hoffman, J Arquilla, D Ronfeldt, M Zanini and B M Jenkins, Santa Monica, CA, RAND, pp 39-84
- Arquilla J and Ronfeldt D, 2001, "Fighting the Network War", *Wired*, 9, 12
- Arquilla J and Ronfeldt D, 2001, "Networks, Netwars, and the Fight for the Future", *First Monday*, 6, 10 Online: http://firstmonday.org/issues/issue6_10/ronfeldt/index.html
- Arquilla J and Ronfeldt D, 2001, "Osama Bin Laden and the Advent of Netwar", *New Perspectives Quarterly*, 18, 4, http://www.digitalnpq.org/archive/2001_fall/osama.html
- Arrighi G, 1994, *The Long Twentieth Century*, New York, Verso

- Arrighi G and Sliver B, 1999, *Chaos and Governance in the Modern World System*, Minneapolis, University of Minnesota Press
- Boulding K E, 1989, *Three Faces of Power*, Newbury Park, NJ, Sage Publishers
- Brunn S D, 1999, "A Treaty of Silicon for the Treaty of Westphalia? New Territorial Dimensions of Modern Statehood", in *Boundaries, Territory, and Postmodernity*, Ed. D Newman, Portland, OR, Frank Cass, pp 106-131
- Buchan G, 1996, *Information War and the Air Force: Wave of the Future? Current Fad?*, RAND, Webpage, Jan 30, <http://www.rand.org/publications/IP/IP149>
- Castells M, 2000, *The Rise of the Network Society*, Malden, MA, Blackwell Publishers
- CERT, 2003, *CERT/CC Statistics 1988-2002*, Web Site, Feb 10, <http://www.cert.org/stats/#incidents>,
- Chroust P, 2000, "Neo-Nazis and Taliban on-Line: Anti-Modern Political Movements and Modern Media", *Democratization*, 7, 1 pp 102-118
- Cilluffo F, Collins J J, Borchgrave, A. d., Goure, D. and Horowitz, M., 2000, *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies*, CSIS, Online PDF, Jan 19, <http://www.csis.org/homeland/reports/defendamer21stexecsumm.pdf>
- Cilluffo F J, 2000, *Cyber Attack: The National Protection Plan and Its Privacy Implications*, Journal of Homeland Security, Webpage, Jan 22, <http://www.homelandsecurity.org/journal/Articles/Cilluffo.htm>

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

Darklaser, 2002, Personal Communication, IM interview, January & February

De Borchgrave A, Cilluffo F J, Cardash S L and Ledgerwood M M, 2000,

Cyber Threats and Information Security: Meeting the 21st Century

Challenge, CSIS, Online PDF, Jan 19, [http://www.csis.org/homeland/](http://www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf)

[reports/cyberthreatsandinfosec.pdf](http://www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf)

Dorobek C J, 2001, *DoD Envisions Virtual Pentagon*, Federal Computer Week,

Webpage, Jan 24, [http://www.fcw.com/fcw/articles/2001/1029/web-](http://www.fcw.com/fcw/articles/2001/1029/web-pent-10-30-01.asp)

[pent-10-30-01.asp](http://www.fcw.com/fcw/articles/2001/1029/web-pent-10-30-01.asp)

Escobar A, 2001, "Culture Sits in Places: Reflections on Globalism and

Subaltern Strategies of Localization", *Political Geography*, 20, 2 pp

139-174

Everard J, 2000, *Virtual States: The Internet and the Boundaries of the Nation-*

State, New York, Routledge

Fisher U, 2001, *Information Age State Security: New Threats to Old*

Boundaries, Journal of Homeland Security, Webpage, Jan 22,

<http://www.homelandsecurity.org/journal/Articles/fisher.htm>

Flint C, 2001, "The Geopolitics of Laughter and Forgetting: A World-Systems

Interpretation of the Post Modern Geopolitical Condition", *Geopolitics*,

6, 3 pp 1-16

- Flint C, 2001b, "A Timespace for Electoral Geography: Economic Restructuring, Political Agency and the Rise of the Nazi Party", *Political Geography* **20** 301-329
- Flint C, 2001c, "Right-Wing Resistance to the Process of American Hegemony: The Changing Political Geography of Nativism in Pennsylvania, 1920-1998", *Political Geography* **20** pp 763-786
- Frank D, 2001, *Clarke Presses Industry on Security*, Federal Computer Week, Webpage, Jan 24, <http://www.fcw.com/fcw/articles/2001/1203/web-clarke-12-05-01.asp>
- Frank D, 2001, *Govnet's Fate Hangs on Policy*, Federal Computer Week, Webpage, Jan 31, <http://www.fcw.com/fcw/articles/2001/1210/pol-govnet-12-10-01.asp>
- Freedman D H and 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 pp 291-307
- Gramsci A, 1971, *Selections from the Prison Notebooks of Antonio Gramsci*, New York, International Publishers
- Gray C S, 1999, *Modern Strategy*, New York, Oxford University Press, Inc.
- Hackivist.com, 2001, *Hackers Versus Crackers*, www.hackivist.com, Oct 12, <http://www.thehacktivist.com/article.php?sid=103&mode=thread&order=0>

- Hafner K and Markoff J, 1995, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, New York, Touchstone
- Hardt M and Negri A, 2000, *Empire*, Cambridge, MA, Harvard University Press
- Himanen P, Castells M and Torvalds L, 2001, *The Hacker Ethic*, New York, Random House
- Hudson A, 2000, "Offshorenness, Globalization and Sovereignty: A Postmodern Geo-Political Economy?", *Transactions of the Institute of British Geographers* **25** pp 269-283,
- Kaldor M, 2001, *New and Old Wars: Organized Violence in a Global Era*, Stanford, CA, Stanford University Press
- Keohane R O, 1984, *After Hegemony*, Princeton, N.J., Princeton University Press
- K-Pax, 2002, Personal Communication, IM interview, February
- Larsen R J and David R A, 2000, *Homeland Defense: Assumptions First, Strategy Second*, Journal of Homeland Security, Webpage, Jan 25, <http://www.homelandsecurity.org/journal/Articles/article1.htm>
- Lenk K, 1997, "The Challenge of Cyberspatial Forms of Human Interaction to Territorial Governance and Policing", in *The Governance of Cyberspace*, Ed. B D Loader, New York, Routledge, 126-135
- Lightblader, 2002, Personal Communication, IM interview, January & February
- Loader B D, 1997, "The Governance of Cyberspace", in *The Governance of Cyberspace*, Ed. B D Loader, New York, Routledge, pp 1-19

- Luke T W, 1998, "Running Flat out on the Road Ahead: Nationality, Sovereignty, and Territoriality in the World of the Information Superhighway", in *Rethinking Geopolitics*, Ed. G O'Tuathail and S Dalby, New York, Routledge, pp 274-294
- Mitchell W J, 1999, *E-Topia*, Cambridge, MA, MIT Press
- Modelski G, 1987, *Long Cycles in World Politics*, Seattle, University of Washington Press
- Molander R C, Riddile A S and 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", in *The People's Liberation Army in the Information Age*, Santa Monica, CA, RAND, pp 175-186
- NetGod, 2002, Personal Communication, IM interview, January
- O'Tuathail G, 1996, *Critical Geopolitics*, Minneapolis, University of Minnesota Press
- O'Tuathail G, 1998a, "Deterritorialized Threats and Global Dangers", *Geopolitics*, 3, 1 pp 17-31
- O'Tuathail G, 1998b, "Postmodern Geopolitics? The Modern Geopolitical Imagination and Beyond", in *Rethinking Geopolitics*, Ed. G O'Tuathail and S Dalby, New York, Routledge, 16-38
- O'Tuathail G, 2000, "The Post Modern Geopolitical Condition", *Annals of the Association of American Geographers*, 90, 1 pp 166-178

President's Critical Infrastructure Protection Board, 2002, *The National Strategy to Secure Cyberspace*, Comment Draft, Washington, D.C.

Phantom, 2001, Personal Interview, December

Pile S, 1997, "Opposition, Political Identities, and Spaces of Resistance", in *Geographies of Resistance*, Ed. S Pile and M Keith, Routledge, pp 1-32

Poster M, 1995, "Postmodern Virtualities", in *Cyberspace/Cyberbodies/Cyberpunk*, Ed. R Burrows and M Featherstone, Thousand Oaks, CA, Sage Publications, pp 79-95

Rheingold H, 2000, *The Virtual Community: Homesteading on the Electronic Frontier*, Cambridge, MA, MIT Press

Ronfeldt D, Arquilla J, Fuller G E and 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 pp 45-61

Ross A, 1991, "Hacking Away at the Counterculture", in *Technoculture*, Ed. C Penley and A Ross, Minneapolis, University of Minnesota Press, pp 107-134

Shroom, 2002, Personal Communication, IM interview, January

Sieberg D, 2001, *Bin Laden Exploits Technology to Suit His Needs*, CNN.com, Sep 22, <http://www.cnn.com/2001/US/09/20/inv.terrorist.search/>

Silver B and Slater E, 1999, "The Social Origins of World Hegemonies", in *Chaos and Governance in the Modern World System*, Ed. G Arrighi and B Silver, Minneapolis, University of Minnesota Press, pp 151-216

- Stephenson W D, 2002, *Homeland Security Requires Internet-Based Thinking -- Not Just Technology*, Journal of Homeland Security, Webpage, Jan 22, <http://homelandsecurity.org/journal/Articles/Stephenson0102.htm>
- Sterling B, 1993, *The Hacker Crackdown*, New York, Bantam Books
- Stinger, 2002, Personal Communication, IM interview, January
- Taylor P J, 1993, "The Last of the Hegemons: British Impasse, American Impasse, World Impasse", *Southeastern Geographer* 33, 1 pp 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, "Embedded Statism and the Social Sciences 2: Geographies (and Metageographies) in Globalization", *Environment and Planning A* 32 pp 1105-1114
- Taylor P J, 2001, "Metageographical Moments: A Geohistorical Interpretation of Embedded Statism and Globalization", in *Odysseys*, Ed. B Denmark and M A Tereault, Yearbook of International Political Economy
- Taylor P J, Beaverstock J and Smith R, 2000, "World-City Network: A New Metageography?", *Annals of the Association of American Geographers*, 90, 1 pp 123-134,
- Taylor P J and Flint C, 2000, *Political Geography: World-Economy, Nation-State, and Locality*, Essex, Prentice Hall

- Vaida B, 2001, *Cybersecurity Chief Pushes Early-Warning System*, Government Executive Magazine, Webpage, Jan 24, <http://www.govexec.com/news/index.cfm?mode=report&articleid=21712>
- Wallerstein I, 1998, "The Time of Space and the Space of Time: The Future of Social Science", *Political Geography* **17** pp 71-82
- Waltz K, 1979, *Theory of International Politics*, New York, Random House
- Ware W H, 1997, *The Cyber-Posture of the National Information Infrastructure*, RAND, Webpage, Jan 28, <http://www.rand.org/publications/MR/MR976/mr976.html>
- Wellman B, 2001, "Computer Networks as Social Networks", *Science* **293** pp 2031-2034
- Wray S, 1998, *Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics*, New York University Web Site, 10/16/2000, <http://www.nyu.edu/projects/wray/wwwhack.html>
- Wray S, 1998, *Towards Bottom-up Information Warfare: Theory and Practice: Version 1.0*, Web Site, 13 Oct 2000, <http://www.nyu.edu/projects/wray/BottomUp.html>
- Wriston W B, 1997, "Bits, Bytes, and Diplomacy", *Foreign Affairs*, 76, 5 pp 172-182
- Youngs G, 1999, "Virtual Voices: Real Lives", in *Women@Internet: Creating New Cultures in Cyberspace*, Ed. W Harcourt, London, Zed Books Ltd. pp 55-68