Research Project AmSt 507 [dellhogge@wsu.edu](mailto:dellhogge@wsu.edu)

Ethics of US CyberWarfare

Research Questions: The newest battlefield on planet Earth is in cyberspace. How does this change the rules of international warfare? Territoriality is shaken to its foundation. Borders are penetrable. Sovereignty is being redefined. National interests take on world-wide meanings. The very definition of *cyber* anything needs to be clarified. *Cyber* appears in the dictionary as *cybernation*: “The use of computers to control automatic processes.” *Cybernetics*: “The comparative study of organic control and communication systems, as the brain and its neurons, and mechanical or electronic systems analogous to them, as robots and computers.”(Random House Websters College Dictionary, 1992). Back then *cyberspace* was simply defined as “virtual reality”. I connect *cyber* to other words in order to make the point that definitions are arbitrary and unsettled at this point in time and space. Morality in cyberspace takes on new parameters. Meanings of property, intellectual and otherwise need to be changed in order to protect the public domain(The Bellagio Declaration in Boyle,1996). The philosophical basis of International agreements on the acts of invasion and conquest come under scrutiny(Ophardt, 2010)(Emmerson, 2013). Indeed, the very foundations of International cooperation are revealed to be currently shaky at best. The economic nature of internet cyberspace, free trade, and globalization are suddenly under review. Recent congressional hearings in the United States reveal a great deal of political concern over the ramifications of cyberwarfare, internet espionage, and the defensive capability of private and government entities.

Russia, China, North Korea, and Iran are identified as cyberenemies of the United States, Israel and the U.K. and the cold war is heating up again. Cyber invasion has already been practiced by Russia in Georgia(Ophardt,2010). China has an army unit devoted to cyberwarfare, and the United States itself has cyber invaded Iran’s nuclear program(ibid). The current sabre rattling by North Korea includes cyberthreats, (although the internet is forbidden to their own people) and Israel and the U.K. are not far behind. Where will this all lead? According to the Revolution in Military Affairs (RMA) concocted by the pentagon at the end of the Cold War(Mirzoeff,2011) this will lead to a new kind of battle, not with tanks and aircraft carriers, missiles and infantry, although the potential for their use is greatly amplified by cyber capabilities, but to an internet web battle, beyond borders, and without adequate defenses in place to prevent the cyber invasion of internet infrastructure. National sovereignty and economic viability are in danger of total collapse to a cyberwarfare invasion from anywhere, anytime, according to the propaganda. Indeed, space and time are in need of philosophical redefinition in the face of cyberwarfare capabilities in the postmodern world. The very essence of understanding the world of nations and trading must come under review. Neoliberal capitalism has taken over the Internet(Solomon,2013) and the US government wants to militarize it. I feel compelled to research and attempt a review of the threat of cyberwarfare in today’s internet environment.

Is cybercrime punishable? Under what laws? By whom? Or can anyone get away with just about anything on the internet. At the criminal level can perpetrators be identified, caught, and tried under due process when cyberspace enjoys the freedoms that it currently enjoys? What about national entities perpetrating cybercrimes against other national entities? When the United States President commands acts of cyberinvasion, as has been done to Iran’s nuclear development program, who will prosecute? When the US pentagon hires thousands of hackers to infiltrate the internet connections of other countries and foreign corporations who will complain and to whom? Indeed, is there a moral conundrum involved in the perpetration of cyberwarfare at all? Or is the internet just a free for all? Apparently the answers to these and other questions concerning cyberspace will be forthcoming given time to work out the details on the international level (Ophardt,2011). Negotiations will include private and government entities and the citizenry of the planet as well. Surely some democratic consensus could be reached eventually that would govern the use of cyberspace to conduct acts of war or espionage against people in general, since all are so intimately interconnected in cyberspace. But is there time? Is there a will to negotiate? Is there a framework, an infrastructure that lends itself to such a project? Is it the United Nations? The Assembly of State Parties (ASP)? Some new entity? Private enterprise? The military industrial complex? The US President on his or her own?

Method: Current academic theoretical treatment of cyberspace is just beginning to take shape in the writings of Harvey, Mirzoeff, Boyle, Coombe, Cassel, Coleman, West, Tsing, Lessig, and others. The postcolonial world is reflected in the writing of Young, Hall, Bhabha, and Giddens. Pulling from these and other sources comments and structures concerning cyberspace’s conceptualization will provide many of the threads of this research project. Literature review must include current events as they appear in media, journalism, and commentary by pundits. For example: Just yesterday, Andrea Germanos, staff writer for Common Dreams, filed a report on the comments of Ben Emmerson, “U.N.special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,” that “If it is lawful for the U.S. to drone al Qaeda associates wherever they find them, then it is also lawful for al Qaeda to target U.S. military or infrastructure where ever (militants) find them… There is a real risk that by promulgating the analysis that is currently being developed and relied upon by the United States they legititimize, in international law, al Qaeda, by turning it into an armed belligerent involved in a war and that makes the use of force by al Qaeda and its associates lawful.”(Emmerson, 2013). This comment reflects the recent McClatchy News report concerning a leaked document that proves the secrecy surrounding U.S. drone strikes in Pakistan is covering up lies and distortions perpetrated by the Obama administration to justify the drone strikes.

Drone warfare is a form of cyberwarfare because it is completely enacted by computer. Thus the use of drones as well as other computer originated attacks constitutes first use of force, something morally questionable, and ethically repugnant. The direct result of justifying al Qaeda and other enemies to take action against the U.S. will be terrorist attacks, either in the form of cyberwarfare or attacks such as the bombing of the Boston Marathon. I argue that the drone attacks on Pakistan, Yemen, and Somalia have radicalized a new consort of terrorists not only in the Middle East but in America as well. Scholarly review of such current information may provide not only event status, but ethical and moral comments salient to understanding cyberwarfare. Field Manual 3-24, 2006, outlines counterinsurgency (COIN) warfare for Commanders in the new world-wide battlefield (Mirzoeff,2011). Countervisuality requires a detailed analysis of this Field Manual and other military documents. The propaganda machine of the United States, Israel, and the U.K. is mobilizing citizenry to support cyberwarfare against perceived enemies, and the number of generals, admirals, and politicians calling for cyber capabilities in defensive posture are growing large. The perception that infrastructure is now defenseless against cyberattack is growing daily with reports from the Department of Homeland Security of cyberespionage, and private enterprise is hollering for protection from foreign corporations who are perpetrating such attacks. The ethical and moral underpinnings of economic conquest need to be included in this research review.

First of all a review of current cyberlaws needs to be conducted. Recommendations for future laws governing cyberspace crime will need to include criminal behavior perpetrated by hackers as well as by government entities. The problem of prosecution is obvious. What International court will be responsible for conducting cyberlaw. “Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow’s Battlefield” by Jonathan A. Ophardt, (A.B. 2003, Princeton University;J.D. Candidate 2010, Duke University School of Law, former Electronic Warfare Officer, United States Air Force), an iBrief available online, suggests the International Criminal Court (ICC) should be reviewing definitions in preparation for prosecution of cybercrime and aggression. International agreements such as The Convention for the Protection of Cultural Property in the event of armed conflict enacted in the Hague on May 14, 1954 (Coombe,1998) need to be rethought.

Territorial borders are not sufficient to control cyberinvasion. The sovereignty of nations as we know them today with internal courts and investigators of criminal behavior, collection of data on crime, and variations in punishment options will need to be Internationalized. Cyberspace is everywhere at once, not constrained by borders or agreements. The commission of cybercrimes may come from a wide variety of places and conditions at once. Or it may be identifiable and the perpetrator simply out of reach or can easily disappear. The rather messy reality of cyberspace leads to a wide variety of ways to cover criminal activity, mislead investigators, or avoid defensive mechanisms.

The proposal currently being funded by the US government is to hire thousands of hackers to work for the Pentagon, the NSA, and DHS, the FBI and etc(Greenwald,2013). Who these people are and how they acquire the expertise to “defend” American infrastructure from cyber attackers is problematic. Hackers as an ethnographic group are notoriously independent (Coleman,2013)). Imagining them as willing to work for the US government to hack the rest of the world’s cyberspace does not seem real. Training students to be prepared for such work is underway according to the LA Times but the numbers simply are not there to put this Pentagon pipedream into place immediately.

Meanwhile billions of US dollars will be directed toward this. Private corporations who stand to benefit from such projects include the entire military industrial complex (Mirzoeff,2011). Profiting from US dominance of cyberspace is a huge project of the neoliberal capitalist economy. To understand the ramifications of cyberwarfare it is necessary to project into the future a scenario of cyberspace that would include almost uncontrolled cyber espionage by large corporations attempting to control the global economy to benefit their bottom line. The ethical and moral conundrums are multiple. Capitalism is poised to exert dominant control of the internet’s business applications, along with control of such infrastructure as the transportation systems, airways, railroads, power grids, waterworks, government entities, and so forth.

Tackling such a weighty problem will require substantive research into definitions of legal usages of words like *territory, sovereign, and offensive/defensive actions*. To picture a world of cyberspace warfare it is necessary to change the current paradigm of international cooperation and globalization. It may seem apparent to western/northern nations that they dominate the eastern/southern nations in cyberspace, as they do in neoliberal development. Indeed, cyberwarfare may seem a logical extension of current imperial policy and capitalist domination. Postcolonial Manifest Destiny. The large corporations that control markets for products of indigenous peoples will continue to control wages and benefits paid out for the services and natural resources of such places as Papua New Guinea(West), and Indonesia (Tsing, 2005).

Cyberspace as a global phenomenon alters little in the lives of much of the world. On the other hand connections through cyberspace are unfolding new parameters for intercommerce and interaction with such places and peoples. Recent appearance in Copenhagen at the world summit against global warming of many indigenous representatives who made the trip at great expense to the most expensive city in the world to voice their demands for mitigating funds for climate change caused by the richer nations is exemplary of changing connections.

Whether their demands ever result in reparations remains to be seen, but the fact that they are voicing their demands is clearly connected to the availability of cyberspace. The Internet as a great leveler of inequality (Cassels) may be a social fantasy, but there is evidence that it may yet become such an instrument of social movement. The Arab spring revolts resulted in changes that were not foreseen before the Internet connections spread viral participation.

Research into the actual policies of the government agencies involved would also include attempts to interview players. Interviewing may be limited by the government secrecy surrounding cyberwarfare. Public relations efforts by government agencies may preclude access to actual documentation. The access journalists now have is so limited that only leaked documents and whistleblowers are available. The current Obama prosecutions of whistleblowers such as Manning as traitors speaks volumes. The shroud of secrecy is tightening around the conduct of this U.S. cyberwar.

Meanwhile, US President Barack Obama has been granted sweeping powers to order preemptive cyber-strikes on any given country, according to anonymous officials involved in a “secret legal review” of US Cyber warfare rules (NYTimes, Feb.19,2013). The secrecy surrounding such preemptive strikes on any given nation does not include oversight by congress or judicial review. “There is no indication that any group of members in Congress or judicial body will have to approve of a preemptive strike before it is carried out”, writes Gosztola at FireDog Lake. “As has become typical, the president wants to be able to conduct war without needing authorization.” No former president of the United States has had such powers. As with the president’s power to conduct drone strikes against countries the US is not officially at war with such as Pakistan, Yemen and Somalia, this expansion of cyberwarfare powers raises the questions of ethics and morality that should govern US warmaking. Appointing Barack Obama and all future presidents to be judge, jury, and executioner when it comes to cyberwarfare, and drone attacks, seems patently UnAmerican.

Arguments and Questions:

The question is, has America become so dominant in the world that it is immune to questions of ethical behavior in warfare against much weaker and demonstrably defenseless countries? If so, then no International forum we know of today can control the conduct of cyberwarfare, let alone prosecute Internet criminality. The fear of cyberwarfare against US economic domination is causing a reactionary preemptive cyberwarfare against perceived enemies that could result in making many more world enemies than we now have to face. A recent attack by Syrian supporters of Hassad on the Associated Press caused the New York Stock Exchange to lose billions of dollars in a few minutes. The money was recovered quickly but the message that such an event could be orchestrated by a group of radical Syrian hackers was clear. Expanding the war against terrorism to cyberspace could drastically alter America’s position in world affairs, making the US a proverbial pariah, the bad guys in a global war.

Economic domination has become the neoliberal hegemony of reality in today’s global economy. The world is dominated by the USA in a lopsided developmental effort that makes the hinterlands of the globe merely natural resource suppliers for capitalism in the US, Canada, and indeed, China. The labor supply of the exploited world seems powerless to negotiate in any meaningful way with the powerful corporations that dominate distribution. Cyberspace has been seen as a hopeful leveler of economic inequality (Casstels,2012) giving equal footing regardless of national borders or cultural difference. Eventual control of the internet by the US will take away that hopeful little bit of hallucination. Indigenous peoples will continue to bear the brunt of global warming, economic exploitation, and oppressive policies (McKibben, 2007).

Cyber warfare has, until now, been relegated to science fiction (Ophardt, 2010). But that has all changed with the militarization of the Internet. President Obama ordered a series of serious attacks on Iranian nuclear capabilities by cyberwarfare capable units of the US military. The cyber battlefield thus became a wide open affair, as foreign nations are now justified by the USA’s first strike use of cyberwarfare. Although Russia previously used cyberwarfare in it’s invasion of Georgia, the use by Obama of cyberwarfare signals the rest of the world that the USA will use cyberspace for preemptive attacks on perceived enemies, without warning and with little provocation. The rules of international war just went out the window. Now anyone with cybercapability can initiate an attack utilizing computers to damage or destroy infrastructure and justify such usage of the internet because the USA did it first.

Hackers have been invading computer networks for decades now and the capability is widespread. Ddos (Distributed Denial of Service) attacks can originate from multiple platforms and the results can be catastrophic. Finding the culprits after the attack can be very problematic and there are currently no international laws governing prosecution or punishment for such an attack (Ophardt, 2010). National laws are, of course, restricted by territoriality and sovereignty. Pursuing international cybercriminals is currently almost impossible, and prosecution by the International Criminal Court is hampered by current regulations and definitions concerning cyberspace (Ophardt, 2010). Laws need to reflect the changes wrought by recent technologies in cyberspace. Dos (Denial of Service) attacks can be accomplished with one computer in a multiplicity of ways. Flooding a computer with demands is most common. The result is a cascade of internet demands that overwhelm a computer system and cause it to crash. Malware is computer code written with harmful intent. It can be installed using a simple e-mail and can cause serious disruption to a network. Enslaving other computers to spread a virus or malware is a common method. Reconstructing the veritable pathways of such a cyberattack can involve worldwide Internet applications and be very frustrating for investigators. Such an attack could conceivably cause sudden loss of control by air and rail systems, reservoirs behind dams, power grids, and much other infrastructure controlled by computers. Nuclear reactors, hospitals, waterworks, and on and on could be cyberattacked.

The various levels of malicious cyber activity include cyber crime, espionage, terrorism, and warfare. Cyber attacks on computer systems controlling infrastructure raise the specter of absolute chaos and generate the most reaction from politicians. Alignment of government entities and private enterprises to prevent, investigate, and prosecute those responsible for cyber attacks seems paramount. The Department of Homeland Security (DHS) fields a team of hackers reacting to reports of cyber attacks. Sharing data with National Security Agency (NSA), Federal Bureau of Investigation (FBI) and other government entities such as the Pentagon is beginning to take place according to testimony given to Congress. More private corporate involvement in cyberdefense is on the rise as more corporations realize their cyber vulnerability. Large corporations such as DOW Chemical are spending millions on cyber defense. Recent congressional hearings on C-Span included representatives from business, and government. Major defense contractors are especially vulnerable to cyber espionage. The joining of government forces with private corporations in defensive efforts is already bearing fruit in the form of shared information about reported cyber attacks.

How does the trope of Foucault’s panopticon fit the paradigm of Internet control as foreseen by the US Military Industrial Complex? Castelle’s book “Networks of Outrage and Hope” spells out the reactionary response of Egyptian power to the uprising known as “Arab Spring”. Attempting to shut down the Internet they perceived as a threat to unify and inform their opposition they pulled the plug on every form of communication they could think of. Still, the uprising found ways of communicating that the government could not control. Seriously dampening the ability to communicate did not stop the uprising, but made it more determined than ever to bring down the regime. Will the US pentagon succeed in hiring enough hackers to control the world wide web? Will the capability to do so insure the action will eventually take place? What about the ethical ramifications of such control? Are we seeing the institutionalization of Orwellian surveillance? The UK already has a closed circuit television camera installed for every 12th citizen (Mirzoeff, 2011).

This research project seeks answers to these and other moral dilemmas created by the willingness of the USA to use cyberwarfare preemptively. The need for transparency in American government planning in this regard is paramount. The President should be clearly within constitutional parameters when exercising cyberwarfare. Congressional oversight should be in place. It is not. Why not? The secrecy surrounding cyberwarfare is ongoing since the Bush administration first embraced the new cyberbattlefield.

Admiral Michael McConnell was formerly Bush’s Director of National Intelligence and has since been in the revolving door of the Military Industrial Complex. As an executive at Booz-Allen, one of the top private security firms, he has continued to orchestrate government-private cooperation in cyberspace. The illegal NSA domestic spying program that implicated telecom giants Verizon and AT&T was his baby (Greenwald, 2013). Privatizing government cyber-espionage and cyberwarfare is his goal now. In a Washington Post Op-Ed he warned that chaos from cyber attacks on American infrastructure could be imminent and that possible missile attack could also be on the table. McConnell’s Op-Ed raised the specter of enemies attacking vulnerable power grids, nuclear facilities, air and ground transportation networks and so forth. The possibilities raised hysterical reactions in some quarters.

The Obama white house followed the McConnell Op-Ed with their own fear mongering decree on cyber-threats, depicting the US as vulnerable to cyber aggression. “President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter…The executive branch was directed to work closely with all key players in US cybersecurity, including state and local governments and the private sector” and to “strengthen public/private partnerships…to implement the recommendations of the Cyberspace Policy Review built on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush.”(Greenwald, 2013).

The rhetoric has only intensified since then. Defense Secretary Leon Panetta, before retiring from office, warned of a cyber Pearl Harbor in rhetoric reminiscent of Condoleeza Rice’s Iraqi “Mushroom Cloud” that ushered in the expensive invasion and 10 year occupation of Iraq. No wonder Congressional hearings on cybersecurity are taking place. The call for massive expenditures on the Pentagon’s plan to hire up to 9,000 hackers to oversee the possible use of the Internet by aggressor nations or terrorist organizations to attack America’s vulnerable infrastructure, meaning the Military Industrial Complex’s Corporate Giants will only enrich government contractors and out of work hackers. It will not guarantee freedom from cyberattack.

The defense of American infrastructure will depend instead on US cyberwarfare in the form of US aggression on perceived enemies in the globalized economic superstructure in preemptive attacks orchestrated by US Military Industrial Complex actors, including the Pentagon, General Alexander at the NSA, Homeland Security, the FBI, and private corporations. This is the Military Industrial Complex warned about in 1952 by former President Dwight D. Eisenhower. It is already obvious from the cyberattack on Iran’s nuclear program that originated in the Obama White house under a cloud of secrecy that the USA is the leading cyberwarfare perpetrator in the world today, and probably in the future. Preemptive warfare in cyberspace is based in the same flawed ethical approach that authorizes drone warfare on Somalia, Pakistan, Yemen, and so on. US aggression, torture, occupation, and immoral use of cyberwarfare are earmarks of the Bush global warfare policy being continued by the Obama administration.

The secrecy surrounding cyber capabilities of the USA is troubling to say the least. The Obama promise of transparency has definitely been compromised when it comes to national defense in general and cybersecurity especially. The usual press leakage and anonymous sources of Washington D.C. politics have been miniscule when it comes to cybersecurity. Perhaps necessarily so. And yet, a national discussion of the ethical and moral ramifications of cyberwarfare is called for. I argue that the Internet has so changed the world that the US government, as world leader, owes it to the world to lead this discussion, rather than to cover it up with fear mongering that amounts to propaganda. The media are complicit in failing largely to respond.

The New York Times ran a story recently that declared China is responsible for an army unit with sophisticated cyberwarfare capabilities that have been employed to attack corporate and government computer networks in the United States. Seen as justification for the US to make huge expenditures on cybersecurity in the form of their own strengthening of cyberwarfare capabilities, this rewarming of the cold war with the “red” threat of communism sadly plays well with the American public. The continued existence of Mutual Destruction in the form of nuclear warheads aimed at each other is not enough for the war mongers of the Military Industrial Complex. They are anxious to employ cyberwarfare in this exciting new battlefield of theirs. The capability of doing so gives Generals and Admirals wet dreams akin to the virtual warfare of video games captivating children (Greenwald, 2013).

In fact, virtualizing warfare is tantamount to selling it to the public (West, 2012) as the next generation of human battle. The cyber battlefield seems like virtual reality without the helmet or joystick. No painful wounding, death, or ultimate sacrifice involved. Only a distant chaos, a melting of the perceived enemies infrastructure, and the resulting domination of US hegemony. Neoliberalism’s ultimate answer to the messiness of globalization, cyberwarfare may indeed result in total domination by the USA, complete with resultant chaos among indigenous peoples, poorer nations, and the rest of the world in general. In my opinion, the continuous capitalist rape of the planet would ensue in this virtual reality until the collapse of the whole cancerous mess and possibly the end of life as we know it. Research is called for, definitely!

Research will need to include extensive literature review, current event analysis, and intense interviews with key players in the Military Industrial Complex, government agencies, and private corporations. Legal expertise in international law will be required, and a team of investigators familiar with hacker culture, military applications of cyberwarfare, and infrastructure networks will need to be assembled.

Funding will need to be found in the private sector. Grants for this type of research may be forthcoming from interested parties, not from government agencies. The wherewithal to actually undertake such a research project is beyond a mere grad student at a state university. I sense, however, that someone somewhere needs to look into this mess further. The powers that be in the pentagon have remodeled warfare into an endless chaotic counterinsurgency that will never end until the USA is absolutely dominant in a colonial world of subservient governments that will bring to fruition Orwell’s 1984 fantasy where “War is Peace” and “Obedience is Freedom”, already visible on US AirForce bases in the form of a billboard I saw recently on Fairchild AFB, Spokane, Washington.

Conclusion:

Nicholas Mirzoeff, in his recent book, “The Right to Look: A CounterHistory of Visuality” offers a countervisuality to this history that is taking place now and I suggest we take him up on it. We still have the “Right to Look” at what is happening in our world, and this cyber battlefield is really happening. This is a continuation of the Rumsfeld doctrine that destroyed and then occupied Iraq. The drone attacks on civilians in far away places controlled by Spec 4’s in Nevada who stare into multiple screens at the virtual reality of death delivery is a result of this policy. The heating up of cold war rhetoric on America’s Fox News is playing well down in Texas, and the certainty of cyber attacks and retaliatory cyber warfare is practically guaranteed unless someone informs the citizenry of the truth, after thoroughly researching free from the constraints of the government propaganda/military public relations apparatus.

“The truth…oh say what is truth?” said Pontius Pilate to Jesus before the crucifixion. In the current world of cyberspace and cybertime the truth may be impossible to ferret out of a White House shrouded in secrecy, a Military Industrial Complex bent on making new fortunes, and a Pentagon determined to conduct endless war in defense of US Imperialism. Economic hegemony requires the naturalization of US corporate domination throughout the world, in words, Neoliberal Globalization. Even a one world government some see as the manifest destiny of the United States.

The internet is definitely a challenge to control freaks everywhere, but especially to the ones that run the Pentagon. Though the names change over time, the policy falling into place remains. It needs to be questioned critically and an informed dialogue ensue that includes the affected peoples of the whole earth. If the visuality of history unfolding is hegemonically controlled without critical countervisuality involved I fear the result will finally be absolute Fascist control without opposition. There needs to be human rights, an end to racism, indigenous rights, a benevolent, inclusive egalitarianism, but where it will come from I cannot foresee.

Research will continue wherever possible, whenever possible, as I see this set of problems as historically important, to say the least. I naturally distrust power, since I have learned through life’s hard lessons that power corrupts, and has a tendency to release the greedy beast in Human Beings. The easy spread of the doctrines of US power through the propaganda machine is especially disturbing in light of the continual warfare being perpetually “played” by the Pentagon’s Generals. The civilian control of our armed forces is rapidly diminishing and the visuality of media made heroes like General McChrystal and General Petraeus portrayed as all-wise on the new battlefield reminds me of the veneration received by Generals in the past, such as George Armstrong Custer. The countervisuality of Phillip Deloria’s book, “Indians in Unexpected Places” comes to mind. General Custer believed his own propaganda and died for it at the hands of aroused natives whose world was threatened by his arrogance. Let us hope that the cyberbattlefield and perpetual war do not dominate US policy in the future, but let us realize they probably will.

Meanwhile I shall try to stay abreast of current events and developments on this subject, the limitations of my unfunded research taken into account. Arousing the kind of money it would take to assemble the needed cohort of knowledgeable researchers to do justice to the many questions raised herein and organize the resulting data into the volumes it would take to contain it all in any useful format is the problem. I realize that. However, having started I cannot stop and I foresee this research project continuing as long as I am able to raise such questions.

I know of no research monies available for research that may seem to sponsors like an attack on American Government. The research may prove my assumptions wrong, and I truly hope so. I hope the President and his advisors are doing the right thing in using propaganda to garner the support of the American public for cyberwarfare in pre-emptive strikes against perceived enemies. It seems certain that they will succeed regardless of what facts can be uncovered about the situation.

Bibliography

* Boyle, James (1996) Shamans, Software, and Spleens: Law and the Construction of the Information Society. Cambridge,Mass. Harvard University Press.
* Castells, Manuel (2012) Networks of Outrage and Hope: Social Movements in the Internet Age. Cambridge, U.K. Polity Press.
* Coleman, E. Gabriella (2013) Coding Freedom: The Ethics and Aesthetics of Hacking. Princeton N.J. Princeton University Press.
* Coombe, Rosemary J. (1998) The Cultural Life of Intellectual Properties: Authorship, Appropriation, and the Law. Durham,N.C. Duke University Press.
* Deloria, Phillip J. (2004) Indians in Unexpected Places. Lawrence, KA. University Press of Kansas.
* Emmerson, Ben (2013) Quoted in Common Dreams.com April 15, 2013, by Andrea Germanos
* Greenwald,Glenn (2013) Pentagon’s New Massive Expansion of Cyber-Security Unit is About Everything Except Defense: Cyber Threats are the new pretext to justify expansion of power and profit for the public-private National Security State. The Guardian, January 28, 2013, U.K.
* Greenwald, Glenn (2013) Three Key Lessons from the Obama Administration’s Drone Lies. The

Guardian, April 12, 2013, U.K.

* McKibben, Bill (2007) Deep Economy: The Wealth of Communities and the Durable Future. New York,N.Y. Times Books.
* Mirzoeff, Nicholas (2011) The Right to Look: A Counterhistory of Visuality. Durham,N.C. Duke University Press.
* Ophardt, Jonathan A. (2010) Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow’s Battlefield. Princeton University.
* Soloman,Norman (2013) Digital Grab: Corporate Power has Seized the Internet. Common Dreams.org
* Tsing, Anna L. (2005) Friction: An Ethnography of Global Connection. Princeton, N.J. Princeton University Press.
* West, Paige (2012) From Modern Productive to Imagined Primitive: The Social World of Coffee From Papua, New Guinea. Durham,N.C. Duke University Press.