Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties

Catherine Hart
Masters student
School of Communication
Simon Fraser University

Introduction

In this paper I seek to explore the way in which the increasing regulation of networked computing through digital controls and surveillance is being justified using a securitizing discourse. I argue that the dominant frame of ‘cybersecurity’ has become one based on national security, due to the potentially debilitating effect that a breakdown of the network would have on society, the economy, the military, and government. This understanding caused President Obama, during his 2008 presidential campaign, to declare the U.S. information infrastructure a ‘strategic asset,’ a move which positions the Internet as a significant issue for the military (Clarke, 2010, 116). Within the Copenhagen School’s perspective on International Security Studies, this is known as a ‘securitizing move’; an attempt to frame something as essential to national security. I seek to examine the application of this securitizing discourse to networked computing and its development into an issue of ‘cybersecurity’ over the past three U.S. administrations. To do this, I will apply the Copenhagen School’s framework to each administration’s official policy on cybersecurity, in order to assess whether the securitization is successful, and what impact proposed responses may have on civil liberties.

Securitization: A Framework for Analysis

A securitization is a speech act which constitutes a ‘referent object’, in this case the state, as threatened in its very existence, and therefore necessitates urgent action (Buzan et al, 1998). The analysis of this process of “securitization” in networked computing involves a three-part process: the identification of a discourse of national security within discussions of networked computing, evidence of the acceptance of this discourse by an audience, and the promotion or uptake of restrictive responses aimed at increasing security. The first part of the process, the mobilization of an existing discourse of national security, relies upon the understanding that “the very utterance of ‘security’ is more than just saying or describing something but the performing of an action,” with the potential to create a new reality (Stritzel, 2007, 362). This is a prominent feature of framing, which Edelman explains allows “the character, causes, and consequences of any phenomenon [to] become radically different as changes are made in what is prominently displayed, what is repressed and especially in how observations are classified” (as cited in Entman, 1993, 54). Therefore scholars of securitization are not concerned with the validity of an asserted threat; their focus, rather, is the action that is facilitated as a result of the acceptance of the validity of a threat. Buzan explains that

> [s]tates, like people, can be paranoid (constructing threats where none exist) or complacent (ignoring actual threats). But since it is the success (or not) of the securitization that determines whether action is taken, that side of threat analysis deserves scrutiny just as close as that given to the material side. (Buzan, 2006, 1102)

The second stage in the process concerns the likelihood that this discourse will be accepted by a wider audience than those advancing the securitization. The ability of an actor to successfully securitize an issue is highly dependent on their position. Security has, to some degree, been institutionalized, as is the case with the military, and therefore "some actors are placed in positions of power by virtue of being generally accepted voices of security, by having the power to define security" (Buzan et al, 1998, 31). Government cybersecurity policy would therefore seem to be an ideal vehicle to mobilize and perhaps also legitimize a securitizing move. Policy represents an administration's official standpoint on an issue which is understood to be a problem, and proposes solutions based on technical knowledge and research. However, as public policy scholar Frank Fischer explains,

> [f]rom the social constructivist perspective... the social and political life under investigation is embedded in a web of social meanings produced and reproduced through discursive practices. Politics and public policy are understood to take shape through socially interpreted understandings, and their meanings and the discourses that circulate them are not of the actors' own choosing or making. (2003, 13)

Public policy therefore contains both a persuasive and a responsive element; it seeks to justify a chosen course of action which is based upon socially interpreted understandings of 'national security'. To use the Copenhagen School's terms, it is both part of the securitizing move, employing a discourse of security, but by its very existence, demonstrates the success of the securitizing move because the issue has been taken seriously enough to warrant an official standpoint and planned response. Assessing how far securitization in policy promotes national security above all other considerations, including civil liberties, is the third part of the process.

By applying a framework of security to an event, it is understood that the issue is one of urgency, and, in the words of Buzan et al, "if the problem is not handled now it will be too late, and we will not exist to remedy our failure" (1998, 26). According to the Copenhagen School's approach, "[t]he invocation of security has been the key to legitimizing the use of force, but more generally it has opened the way for the state to mobilize, or to take special powers, to handle existential threats" (ibid, 21). If a securitization is successful, an audience will tolerate violations of rules that would otherwise have to be obeyed, for example the restriction of free speech, or freedom from unreasonable search and seizure. By its very definition, a framework selectively calls attention to certain aspects of reality, and therefore ignores or omits others (Entman, 1993, 54). A security framework privileges security above all other concerns, sometimes to the detriment of civil liberties. It is commonly understood that to attain security, a little freedom must be given up, but how much freedom is under debate. It is not yet clear whether the security arguments of the U.S. military, the intelligence community, and more hawkish members of government will result in the *hypersecuritization* of cyberspace—to use Barry Buzan's term for the mobilization of exaggerated threats and excessive countermeasures (2004, 172)—or whether a more measured view, taking into account civil liberties and the positive potential of the Internet, will win out.

To explore these three stages, I will begin by outlining the development of "national security" as a securitizing discourse, and how it has been applied to the Internet. Then I will look to major cybersecurity policy developments over the past three administrations in order to highlight official discourses of security, namely, the Clinton Administration's *Critical Foundations: Protecting America's Infrastructures* (1997), the George W. Bush Administration's *National*

Strategy to Secure Cyberspace (2003), and the Obama Administration's *Cyberspace Policy Review* (2009). I will illustrate how the threats and the proposed responses have evolved over time, and the degree to which the securitization can been said to have been accepted through the targeting of different audiences, from policy-makers to critical infrastructure and industry, to the general public. I conclude by asking, what responses are being justified by the acceptance of the existence of threats to the nation through networked computing? What consideration, if any, is given to the impact these responses may have on civil liberties?

The Discourse of National Security

Traditionally, national security has been the purview of the military, and threats have appeared in the form of adversarial states through warfare, and perhaps from within the state through civil war. Buzan and Hansen identify several bodies of literature in war studies, military and grand strategy, and geopolitics which focus on these traditional understandings of security and extend back to before the Second World War (2009, 1). However a distinct body of literature concerned specifically with security began to develop after 1945, and paved the way for a broader study of the concept of security after the Cold War. They explain that this literature was distinct because "it took security rather than defence or war as its key concept, a conceptual shift which opened up the study of a broader set of political issues, including the importance of societal cohesion and the relationship between military and non-military threats and vulnerabilities" (ibid).

This conceptual shift was also used to explore the new problems presented during the Cold War of the avoidance of the deployment of weapons. The use of nuclear weapons on Hiroshima and Nagasaki during the Second World War both realized and ended 'total war'; mutually assured destruction or 'MAD' ensured that total war was no longer viable in nuclear-armed states (Gray, 1997, 168). Hannah Arendt calls this shift "a radical change in the very nature of war through the introduction of the deterrent as the guiding principle in the armament race" (Arendt, 1965, 6). This also prompted the dissolution of any kind of real or imagined separation between the civilian and military domains, and expanded the concept of security into a more civilian enterprise, a third major focus of the new security studies field. Civilians would be the majority of the victims in a nuclear attack, but in another sense, civilian experts, from physicists to economists to sociologists were needed to expand military knowledge in this new war-avoiding climate of deterrence (Buzan & Hanson, 2009, 2). The role of civilians has grown even more important to current military efforts due to the increasing reliance on research and development as the military struggles to come up with more intelligent and effective weapons to accommodate these shifts in warfare.

Traditional concepts of national security were again challenged by the fall of the Soviet Union and the end of the Cold War. Buzan argues that

> [w]hen the Cold War ended, Washington seemed to experience a threat deficit, and there was a string of attempts to find a replacement for the Soviet Union as the enemy focus for US foreign and military policy... which for more than 40 years had created a common cause and a shared framing that underpinned US leadership of the West (2006, 1101).

At a time when the US held the position of the only remaining superpower, with no other nation possessing the military might to challenge it, the traditional understanding of security as being state and militarily-oriented was shaken by the events of September 11, 2001. The devastating attacks, targeting civilians and carried out not by a rogue or enemy state but by terrorists, created a new concept of security in which everyone was a potential threat, and everyone was therefore suspect. Providing a solution to the threat-deficit, Lyon argues that "[a]nti-terrorism initiatives pick up where the Cold War rhetoric and attitudes left off, replacing the old "Communist" bugbears with "terrorist" ones (2003, 7).

As issues of national security have expanded beyond traditional understandings of the military and warfare, and the invocation of the Global War on Terror has created a climate of constant, low-level threat, the response has been an increase in regulation and surveillance. Agamben explains the effect of this shift on the way in which nations are governed, documenting the gradual emancipation of a 'state of exception' from periods of warfare, through the declaration of this state of emergency in times of economic crisis, strikes, and social tensions. The result of this expansion of 'exceptional circumstances' has been that "the declaration of the state of exception has gradually been replaced by an unprecedented generalization of the paradigm of security as the normal technique of government" (2005, 14). The state of exception has now become the rule (Benjamin, 2003 392).

The framework of national security has therefore been expanded to encompass a wider range of threats, but still invokes pre-existing schemata. As a result, non-military threats have been framed in traditional security terms by politicians for the last several decades, for example the 'war on drugs', as a means of justifying increasing government regulation and control (Buzan, 2006, 1104) and it is into this framework that cyber security has been added (Nissenbaum, 2005; Nissenbaum & Hansen, 2009; Bendrath, 2003; Bendrath et al, 2007; Saco, 1999). As explained by Myriam Dunn, when addressing cybersecurity, states usually focus on the protection of critical infrastructure, which includes information systems and telecommunications, energy and utilities, transport, and finance (2007, 87). Since being connected to computer networks, these facilities have become vulnerable to attack, as they could be hacked into by outsiders and damaged. At the same time, the Internet "challenges conventional ways of thinking about space, sovereignty, and security" due to its transgression of national borders (Saco, 1999, 262), and such a challenge to state authority through the "blurring of traditional boundaries" has prompted great anxiety from security advisers (ibid, 263). The inability to control the traffic which crosses into U.S. cyberspace, combined with the integration of information systems into all areas of life including critical infrastructure and the military, play into fears about asymmetrical threats. That is to say, with very little risk or investment, a weaker adversary could exploit U.S. information dependence and strike at this weak point while avoiding the nation's military strength (Dunn, 2007, 93). A concern with this threat is clear throughout cybersecurity policy, as I will show in the analysis of securitization in three key documents from the last three administrations.

Securitization in Policy

Nissenbaum and Hansen propose that institutional developments such as the Commission on Critical Infrastructure Protection under President Clinton, and President Bush's formulation of *The National Strategy to Secure Cyberspace* in 2003 are evidence of successful securitization (2009, 1157). I echo these sentiments, and would argue that a closer examination of these institutional developments reveals an ongoing process of securitization, in which the securitizing move is continually made towards different target audiences, and the success of the overall securitization can be seen to increase over time with each audience's acceptance. The illustration of this gradual shift has informed my selection of the policy documents under consideration, as I will explain.

Audience Acceptance

A securitization cannot be said to have been successful unless the discourse has been accepted by the audience, otherwise it can only be seen as a "securitizing move". The first significant attempt at achieving acceptance was in a report written by the President's Commission on Critical Infrastructure Protection, called *Critical Foundations: Protecting America's Infrastructures* (CF). It is on this report that the Clinton Administration's cybersecurity policy, *Presidential Decision Directive 63* (PDD 63) was based. The policy document itself is brief—only 15 pages—which is in keeping with its position as a first attempt at articulating cybersecurity policy. However the report is a much more in-depth exploration of the issues, and it will be one of the documents under consideration. While its audience differs from the other two policy documents I have selected, in that it addresses government officials and policy makers rather than a broader public, it should be understood as situated at the beginning of the securitization process, when little was known or understood about the issue, meaning that policy makers first needed to be convinced of its importance. The *National Strategy to Secure Cyberspace* (NSSC) was written half a decade later, by which time, according to PDD 63, the security of critical infrastructure should have been achieved, but this had not been the case. Internet penetration in the U.S. was much higher, the networking of critical infrastructure much greater, and there was a greater awareness and acceptance within government of the vulnerabilities in national security which could be exploited through the Internet. Therefore a much more concerted effort is made in this document to communicate this knowledge not only to government and industry, but to the general public, whose use of this digital infrastructure could have a direct impact on the security of the nation.

The NSSC superseded PDD 63, and gave responsibility for the coordination of national efforts to protect critical infrastructure to the new Department of Homeland Security, situating cybersecurity firmly in the context of counter-terrorism efforts. This was followed by the *Comprehensive National Cybersecurity Initiative* (CNCI) of 2007, "which is neither comprehensive, nor national" and focuses on securing government networks (Clarke, 2010, 115). It is also classified, except for a one-page outline released in 2010, and thus will not be examined in this paper. Finally, the most recent document under consideration is the *Cyberspace Policy Review* (CPR) of 2009 which does not offer much in the way of new policy, but rather reaffirms existing efforts, and places slightly greater emphasis on public awareness-raising.

The securitizing move can most clearly be seen in the documents in the sections entitled, "A Case for Action" (President's Committee on Critical Infrastructure Protection, 1997, 1; Department of Homeland Security, 2003, 5; National Security and Homeland Security Councils, 2009, 1). However, the fact that this persuasive element is given the entire first part of the document in CF, a chapter in the NSSC, and only a paragraph in CPR suggests a shift in the need for persuasion, perhaps indicating that, between the release in 1997 of CF, one of the first official reports on the cyber-threat to national security, and the writing of CPR over a decade later, the protection of the Internet had been more generally accepted as an issue of national security, at least by policy-makers and those in power. However, the emphasis placed by all three documents on public "awareness raising" and education with regard to the cybersecurity threat suggests that wider audience acceptance had not yet been achieved. They note two main areas of concern: the need to improve training in cyber security to produce a greater number of experts, and a lack of understanding of the issues by the American public (PCCIP, 1997, 69; DHS, 2003, 37; NSHSC, 2009, 13).

An increase in efforts to promote the acceptance of the securitization by the general public can be seen through a comparison of the documents; CF does not appear to address the general public in any concerted way, probably due to the fact that its target audience is composed of government officials and policy-makers. It therefore makes appeals to government and industry, emphasizing the importance of their mutual cooperation in promoting national security. The NSSC, on the other hand, makes an explicit outreach to the American public, explaining that its purpose is "to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society" (DHS, 2003, vii). The document thus emphasizes the responsibility of the individual to the nation, and also the fact that the decision to participate belongs to the individual, rather being forced on them by the government. The CPR takes a more focused approach, stating that government must "inform and persuade the public about the importance of cybersecurity" (NSHSC, 2009, 14). The word "inform" suggests not only giving the public the facts and telling them what is true, but also determining what that truth is. Similarly "persuade" suggests a need or desire to bring public opinion in line with that of the government. This is, on the one hand, necessary in order for cybersecurity to be successful, and on the other, necessary for *this particular strategy* of cybersecurity to be successful.

Referent Object

In any securitization there is a referent object, or that which is threatened, which in traditional security studies is usually the state. This is clearly the case in the policy documents under consideration, as is evidenced by their constant evocation of national security. More specifically, however, the referent object is the critical infrastructure upon which the nation relies for proper functioning. CF refers to critical infrastructure as **"**the life support systems of our nation" (PCCIP, 1997, 5) and "the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society" (11). This document suggests that the various critical infrastructure sectors are vulnerable because they are so interconnected through networked computing.

In the NSSC, I would argue that networked computing becomes a referent object in and of itself, rather than just a cause of vulnerability, as is evidenced by this opening statement, which is worth quoting at length:

> Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country... Thus, the healthy functioning of cyberspace is essential to our economy and our national security (DHS, 2003, vii).

In this statement, various elements critical to a functioning society are said to be at risk, but this risk comes from the threat posed to cyberspace, thus, the Internet is positioned as a referent object of security. The CPR makes this even more explicit, opening with the lines, “[c]yberspace touches practically everything and everyone... But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights” (NSHSC, 2009, i). Critical infrastructure, outside of digital infrastructure, is not mentioned until seven pages in, and then extremely briefly. This shift in focus can be most obviously seen in the titles of the documents: ‘*Critical Foundations*: Protecting America’s *Infrastructures*’ versus the ‘National Strategy to Secure *Cyberspace*’ and the ‘*Cyberspace* Policy Review." This shift in emphasis is significant because the area which requires protection is also the area which will need to be most tightly controlled. Rather than focusing on directly securing the critical infrastructure on which the nation depends, these policies seem to promote—rhetorically at least—the securitization of the method through which these sectors could be attacked. While this makes strategic sense, as it is easier to safeguard a network than a large number of disparate critical facilities, it could also have worrying implications for civil rights, as these channels are not only used to connect infrastructure, but also to allow communication and to promote free speech, while maintaining privacy and personal security.

Existential Threat

The key component of a securitization is that a dire threat is posed to the referent object which will ultimately result in its destruction. An existential threat to the nation is usually posed in terms of a threat to sovereignty. Critical infrastructures and the computer networks which connect them must therefore not simply be understood as important to the functioning of the nation, but essential. Critically, Buzan et al suggested in 1998 that cybersecurity was a failed securitization because, in their view, a cyber attack would not cause cascading effects throughout society, but rather would only be felt within the computer field (1998, 25). Nissenbaum and Hansen questioned this view in 2009, as networked computing has become increasingly embedded in all areas of society, and in fact Rachel E. Yould suggests that “IT may be the common underlying factor upon which all security sectors are destined to converge” (as cited in Hansen & Nissenbaum, 2009, 1157). CF illustrates this existential threat well, stating “the nation is so dependent on our infrastructures that we must view them through a national security lens. They are essential to the nation’s security, economic health, and social well being. In short, they are the lifelines on which we as a nation depend” (PCCIP, 1997, 11).

The NSSC refers to digital infrastructure as “essential to our economy, security, and way of life” (DHS, 2003, iii) and therefore aims to “reduce our Nation’s vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them” (viii).

The existential threat is legitimized by references to traditional threats to national security, such as war and terrorism. This is important because the cyber-threat is entirely hypothetical, as is the case in any securitization. Buzan et al explain that security arguments “are about the future, about alternative futures—always hypothetical—and about counterfactuals. A security argument always involves two predictions: What will happen if we do not take "security action’... and what will happen if we do” (1998, 32). Drawing parallels with past examples to justify a security action, and to threaten disaster if no action is taken, gives legitimacy to the argument that a government should act pre-emptively, rather than wait for disaster to strike. To this end, CF draws comparisons between a “cyber attack” and attacks using chemical, biological, and nuclear weapons (PCCIP, 1997, 14), and all three documents invoke the public memory of specific past attacks or threats to the security of the U.S., from Pearl Harbour to the Cold War to the Oklahoma City bombings and 9/11. The links between the 9/11 terrorist attacks and potential future cyber attacks are, unsurprisingly, drawn most clearly in the NSSC, which was written as a component of the *National Strategy for Homeland Security*, part of the regulation responding to the terrorist attacks of September 11, 2001. A clear but largely imaginary link is drawn between the terrorist attacks and potential future cyber attacks in the following statement:

> [u]ntil recently overseas terrorist networks had caused limited damage in the United States. On September 11, 2001, that quickly changed. One estimate places the increase in cost to our economy from attacks to U.S. information systems at 400 percent over four years. While those losses remain relatively limited, that too could change abruptly (DHS, 2003, 10).

The imperative to act sooner rather than later is then emphasized by the line, "[c]yber attacks can burst onto the Nation's networks with little or no warning and spread so fast that many victims never have a chance to hear the alarms" (DHS, 2003, 7). This is consistent with Nissenbaum and Hansen's identification of the establishment of a complacent audience that is unaware of the impending danger, which is another key trope of securitizing discourse (2009, 1161). This logic can be used to persuade policy-makers of the greater good that can be accomplished by placing restrictions on the Internet, even if doing so potentially infringes on civil liberties. As Arnold Wolfers explains, 'national security' is an ambiguous concept for which there are different understandings. This will therefore prompt different responses, which could be "praised for their self-restraint and the consideration which this implies for values other than security [or] they may instead be condemned for being inadequate to protect national values" (Wolfers, 1952, 501). It is perhaps better to err on the side of caution, and support more restrictive policies, than to be seen as having risked national security and a repeat of the physical and psychological damage of 9/11.

Successful Securitization?

Having reviewed the securitizing discourse in the documents, I would suggest that *Critical Foundations* is a securitizing move, but perhaps not a successful securitization. Using the Copenhagen School's criteria, it cannot be seen as generating enough immediacy and salience to promote more general audience acceptance. The report repeatedly states that no evidence was found of an impending attack (PCCIP, 1997, 5), and that

> [p]hysical means to exploit physical vulnerabilities probably remain the most worrisome threat to our infrastructures *today*. But almost every group we met... emphasized the importance of developing approaches to protecting our infrastructures against cyber threats ***before*** they materialize and produce major system damage (PCCIP, 1997, 5).

While a threat is suggested, the emphasis on being prepared *before* threats materialize has the unintended effect of confirming that this is not an immediate issue, but may be at some point in the future. While the report did prompt President Clinton to pass *Presidential Decision Directive 63* the following year, in terms of actionable response, the author of the document, Richard A. Clarke, calls it "toothless" (Clarke, 2010, 109). Conversely, the NSSC is much more emphatic that these threats are very much present today. It suggests that the reason we have not yet experienced a nationally debilitating cyber attack is due to the high technical sophistication needed to carry out such an attack (DHS, 2003, viii). It then assures the audience that “[t]here have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities” (ibid), thereby suggesting that smaller-scale attacks have occurred, and will only become more effective with time. The CPR goes even further, outlining specific cyber-incidents, disruption and damaged caused, and estimated financial losses (NSHSC, 2009, 2).

The increase of a sense of urgency in the documents, the institutionalization of cybersecurity efforts, and the targeting of progressively wider audiences seems to suggest a gradual acceptance, at least within government, of the securitization of cyberspace. Therefore in conclusion, I ask what responses are being justified by the acceptance of the need to increase cybersecurity, and what consideration, if any, is given to the impact these responses may have on civil liberties?

Responses to Securitization and Areas of Further Research

Perhaps surprisingly, given the level of urgency with which the subject is addressed, all three documents hold firm to the American belief in federal non-intervention in the private sector, and eschew the regulation of industry. They recommend instead a response based on increased coordination and information sharing with the private sector, alongside a public awareness-raising campaign, and the government leading by example. In an effort to ensure that this public-private partnership is “genuine, mutual and cooperative,” *Critical Foundations* recommends that “the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector” (PCCIP, 1997, 3). Rather, it is suggested that financial incentives should be used to encourage the desired behaviour (4). The NSSC further addresses the balance between the public and private, and the importance of non-intervention, stating that “[t]he federal government should likewise not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks’’ (DHS, 2003, 11). Little attention is therefore given by the documents to civil liberties because little is needed, beyond ensuring that the promoted ‘information sharing’ respects privacy rights, so that “[c]onsumers and operators... have confidence that information will be handled accurately, confidentially and reliably” (PCCIP, 4). The CPR also suggests the designation of a privacy and civil liberties official to the National Security Council cybersecurity directorate to address any privacy concerns (NSHSC, 2009, 37).

However there is evidence of some dissatisfaction among security advisors with this approach. To Richard Clarke, these efforts at cybersecurity have been an “unmitigated failure” (Clarke, 2010, 104). Serving as the National Coordinator for Security, Infrastructure, and Counter-Terrorism under Clinton and the Special Advisor to the President for Cybersecurity under George Bush, he is also the author of PDD63 and headed the team that wrote the NSSC. He has long been an advocate of more stringent controls over cyberspace, and in his book, *Cyber War: The Next Threat to National Security and What to Do About It*, he suggests several much more intrusive and restrictive methods of cybersecurity. While military networks are governed and protected by U.S. Cyber Command, and the DHS has responsibility for dotgov networks, the safety of public networks is left to industry, and he does not trust industry to regulate itself, due to the fact that the information sharing and voluntary measure approach has been government policy for over a decade, but this has not protected cyberspace from a series of major incidents which have affected its proper functioning (Clarke, 2010, 113-112). He complains that, during the Bush Administration especially, the White House did not taken cybersecurity seriously enough, stating that "[n]o regulation and no decision-making authority meant little potential for results" (109).

Amid these security failures, he highlights two examples of successful methods of network security in support of the argument for increased regulation. Firstly, he explores the possibility for the extension of a DHS system called "Einstein," currently limited to dotgov networks, to the private sector. The system monitors network traffic flows, detects intrusions and malware, and "will soon attempt to block Internet packets that appear to be malware" (Clarke, 2010, 121). Focusing on monitoring and safeguarding the network rather than the individual facilities that are connected by the network makes strategic sense, as there are too many facilities to defend, and the distaste for regulation discourages any attempt at government involvement in industry security (159). However, allowing the government to conduct deep packet inspection of public network traffic raises obvious concerns for privacy and civil liberties. Secondly, and of greater concern, he seems to advocate an Internet "kill switch". He cites the successful example of John Hopkins University's Advanced Physics Laboratory, which, upon discovering in 2009 that large amounts of data were being stolen from its network, simply "pulled the plug and isolated its entire network" while they located the source of the attack (ibid, 127). He also speaks in somewhat envious terms of the comparative cyber-advantage China enjoys over the U.S. due to their almost total control of the nation's Internet access, and their ability to disconnect the nation's Internet from the rest of the world (146).

His support for the idea of 'pulling the plug' on a network is concerning because similar legislation has come before Congress in recent years. The *Protecting Cyberspace as a National Asset Act* of 2010 (PCNAA), currently under consideration by the Senate, would give the federal government far-reaching powers during a 'cybersecurity emergency' over any private company that "relies on" the U.S. information infrastructure (McCullagh, 2010, para.6). The bill would give the DHS the authority to direct these private companies, which could be Internet service providers, search engines, or software firms, to comply with its chosen course of action to preserve the U.S. information infrastructure, even if this means disconnecting these companies, and by extension their subscribers, from the Internet. The American Civil Liberties Union and other civil rights and privacy groups have voiced concern about the lack of criteria for establishing the scope of the legislation's authority, the lack of an explicit definition of what constitutes a 'cybersecurity emergency', the potentially endless period of time for which these emergency measures can be in effect, and the potential chilling of free speech which could occur if, during such a state of emergency, people were no longer able to access the Internet for information and to voice dissent (ACLU, 2010, 1-2).

In conclusion, given this context, it would appear that while policy may not in itself restrict civil liberties, it promotes the discourse which could facilitate the enactment of restrictive laws. A focus on cybersecurity 'awareness raising' with the public can only increase the securitizing discourse around these issues. At the same time, a growing frustration is clear among security advisors with the lack of regulation and the inaction of cybersecurity policy, despite the protection it offers to civil liberties. Regulation might be an unpalatable word for both the left and the right in the U.S., but it is generally accepted that in cases of national emergency, it is sometimes necessary for the government to step in. The history of the discourse of 'national security' has demonstrated that exceptional responses can be justified when this discourse is mobilized, and Agamben has warned of the shift in government towards the issuing of exceptional laws rather than the declaration of a state of exception (2005, 21). The PCNAA is a prime example of such an exceptional law which could be employed during a 'state of emergency' vaguely defined as a "risk of disruption" to cyberspace, with virtually no limit on its scope or length of effect (ACLU, 2010, 1-2). As the securitization of cyberspace achieves success with wider audiences, I predict an increase in surveillance and control as governments accept the failure of voluntary measures, and legislate emergency responses.

References

ACLU (2010, June 23). Civil Liberties Issues in Cybersecurity Bill [Letter to Senators Lieberman, Collins and Carper]. *Center for Democracy and Technology*. Accessed December 7, 2010 at http://www.cdt.org/files/pdfs/20100624_joint_cybersec_letter.pdf

Agamben, G. (2005) *State of exception*. (K. Attell, Trans.). Chicago: University of Chicago Press.

Arendt. H. (1965). *On Revolution*. Viking Press: New York.

Benjamin, W. (2003). *Selected Writings Volume 4 1938-1940* M Jennings (Ed.) Cambridge, MA: Belknap Press of Harvard University Press.

Buzan, B. (2004). *The United States and the great powers: World politics in the twenty-first century*. Cambridge: Polity Press

Buzan, B. (2006) Will the 'global war on terrorism' be the new Cold War? *International Affairs* 82(6), 1101–1118.

Buzan, B. and Hansen, L. (2009). *The Evolution of International Security Studies*. Published Cambridge: Cambridge University Press.

Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: A New Framework For Analysis*. Boulder: Lynne Rienner.

Bendrath, R. (2003). The American cyber-angst and the real world – any link? In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. New York: The New Press, 49-73.

Bendrath, R. (2007). From cyberterrorism, to cyberwar, back and forth; how the United States securitized cyberspace. *International relations and security in the digital age.* Johan Eriksson and Giampiero Giacomello, (Eds.). New York : Routledge.

Clarke, R.A. & Knake, R.K. (2010). *Cyber War: The next threat to national security and what to do about it.* HarperCollins Publishers: New York.

Department of Homeland Security (2003). *The national strategy to secure cyberspace: [electronic resource] draft for comment / The President"s Critical Infrastructure Protection Board.* The Board, Washington, D.C. Retrieved from http://purl.access.gpo.gov/GPO/LPS22941

Derian. D.J. (1993). The Value of Security: Hobbes, Marx, Nietzsche, and Baudrillard. In D. Campbell and M. Dillon (eds.), *The Political Subject of Violence*. Manchester University Press: Manchester.

Dunn, M. (2003). Securing the Digital Age. In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. New York: The New Press, 85-105.

Entman, R. (1993). Framing: Towards clarification of a fractured paradigm. *Journal of Communications* 43(4): 51-58.

Fischer, F. (2003). *Reframing Public Policy*. New York, NY: Oxford University Press.

Gray, C.H. (1997). *Postmodern War: The New Politics of Conflict*. London: Routledge.

Hansen, L. & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53: 155–1175.

Lyon, D. (2003). *Surveillance After September 11.* Cambridge: Polity Press.

McCullagh, D. (2010, June 10). Senators propose granting president emergency Internet power. *Cnet News*. Accessed December 7, 2010 at http://news.cnet.com/8301-13578_3-20007418-38.html#ixzz16pzR4uPv

National Security and Homeland Security Councils (2009). *Cyberspace policy review [electronic resource]: assuring a trusted and resilient information and communications infrastructure*. Executive Office of the President of the United States, Washington, DC. Retrieved from http://purl.access.gpo.gov/GPO/LPS118258

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology* 7 (2): 61-73.

President's Commission on Critical Infrastructure Protection. (1997). *Critical foundations: [electronic resource] protecting America's infrastructures.* The Commission, Washington, D.C. Retrieved from http://www.fas.org/sgp/library/pccip.pdf

Saco, D. (1999). Colonizing Cyberspace: "National Security" and the Internet. In *Cultures of Insecurity: States, communities, and the production of danger*. J. Weldes, M. Laffey, H. Gusterson and R. Duvall, (Eds.). Minneapolis: University of Minnesota Press, 261-291.

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations* 13(3): 357-383.

Smythe, D. (1986). On the Political Economy of C3I. In J. Becker, G. Hedebro, and L. Paldán (Eds.). *Communication and Domination: Essays to honor Herbert I. Schiller.* Ablex Publishing Corporation, Norwood, New Jersey.

Wæver, O. (1995). Securitization and Desecuritization. In Ronnie Lipschutz (Ed.). *On Security*. New York: Columbia University Press, 46-86.

Wolfers, A. (1952). National security as an ambiguous symbol. *Political Science Quarterly*, 67(4): 481-502.