Securing Freedom: A media framing analysis of cybersecuritization

by

Catherine Elizabeth Hart

B.A., University of Birmingham (UK), 2007

Thesis Submitted In Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Communications
Faculty of Communication, Art and Technology

SIMON FRASER UNIVERSITY

Fall 2012

Approval

Name:	**Catherine Elizabeth Hart**
Degree:	**Master of Arts (Communications)**
Title of Thesis:	***Securing Freedom: A media framing analysis of cybersecuritization***
Examining Committee:	**Chair:** J. Adam Holbrook, Adjunct Professor

Andrew Feenberg
Senior Supervisor
Professor

Firstname Surname
Supervisor
Assistant/Associate/Professor

Richard Smith
Supervisor
Professor

Peter Chow White
Supervisor
Assistant Professor

Gary McCarron
Internal Examiner
Assistant/Associate/Professor
School of Communication

Date Defended/Approved: 2012-11-14

Partial Copyright Licence

Abstract

The integration of networked computing into all areas of U.S. society has resulted in growing concern over the need for secure systems and the importance of freedom of access. This thesis explores the discursive struggle among security professionals over the best way to guarantee this security, the related competition for resources in the burgeoning cyber-industrial complex, and the fate of civil liberties in this turf war. The Copenhagen School's Securitization Theory goes some way to exploring how support for certain approaches is rhetorically mobilized, however it is limited in its exploration of audience response. The theory can therefore be enhanced by looking at the framing and agenda-setting function of the media in this process, both as an audience and as a method of disseminating security arguments. This approach allows for a consideration of the conditions specific to the cybersecurity case—both internal and external to the speech act—that facilitate audience acceptance.

Keywords: Cybersecurity; Securitization Theory; Media Effects; Framing; Google; United States of America

Dedication

For N, for your patience; and for Steve.

Acknowledgements

I would like to thank my supervisory committee Andrew Feenberg, Richard Smith, and Peter Chow-White for their direction and feedback, as well as Gary McCarron for his insight and advice.

The members of the Applied Communication and Technology Lab have given me countless hours of advice, inspiration, and camaraderie. Special thanks to Milan Singh and Roy Bendor, without whom this thesis might never have been finished.

My graduate cohort has likewise been a wonderful source of knowledge, assistance, and insight throughout my masters; thanks to Jeff Whyte, Scott Timcke, Ben Woo, Maggie MacAulay, and Marcos Moldes.

Thanks and love to my parents for their support and unending optimism.

Table of Contents

List of Figures

List of Acronyms

ARPANET	Advanced Research Projects Agency Network
BBS	Bulletin Board System
CNCI	Comprehensive National Cybersecurity Initiative
CPR	Cyberspace Policy Review
CSIS	Center for Strategic and International Studies
ISS	International Security Studies
NIPRNET	Unclassified but Sensitive/Non-classified Internet Protocol Router Network
NSA	\National Security Agency
NSSC	National Strategy to Secure Cyberspace
OS	Operating System
PC	Personal Computer
PCCIP	President’s Commission on Critical Infrastructure Protection
SIPRNET	Secret Internet Protocol Router Network
TCP/IP	Transmission Control Protocol/Internet Protocol
UN	United Nations
Y2K	Year 2000 (Millennium Bug)

Glossary

Arab Spring	A series of pro-democracy uprisings in the Middle East and North Africa beginning in December 2010
Asymmetric Threats	A theory of warfare which holds that a much weaker force can beat a stronger opponent if it can counter with weapon that exploits a weakness
Backbone	The main data routes between large networks on the Internet; the network underlying, connecting, or supporting smaller networks
Computer Security	Keeping a computer system safe from attacks which threaten the availability, integrity, or confidentiality of that system
Constructivism	An approach that emphasizes the interpretative nature of social reality and its distortion depending on that interpretation
Content Analysis	A quantitative method of studying the content of communication
Copenhagen School	A school of International Security Studies who take a constructivist approach to security
Critical Infrastructure	National assets that are essential to the functioning of society, for example information systems and telecommunication, energy and utilities, transport, and finance
Cyber-Industrial Complex	A country's computer security industry that has close ties to the military, similar to the military-industrial complex
Cyberattack	A networked computer-based attack aiming at altering, stealing, or destroying data
Cybersecuritization	Attempts to increase the security of the Internet, or and increasing tendency to the Internet as something that should be secured
Cybersecurity	An approach to computer security that is concerned with national security
Cyberspace	The series of networks collectively referred to as the 'Internet'
Cyberterrorism	The use of networked technologies for terrorism
Cyberwar	The use of information and communication technologies in warfare; particularly the use of networked technologies
Existential Threat	A threat to a referent's very existence
Facilitating Conditions	Circumstances both external and internal to the security speech at that increase the likelihood of its acceptance
Fibreoptic	The optical fibre used in the physical cables that make up networks
Focusing Event	Events which allow a condition to be seen as a problem

	necessitating action
Framing Analysis	A qualitative method of studying the content of communication
Functional Actor	Actors who influence the dynamics of the security field without being the ones to actually perform the security speech act
Google	A major Internet company best known for its search engine
Hacker/Hack	A person who is skilled at computer programming; often used to describe the unauthorized accessing or changing of computer code
Hypodermic Needle	The theory that audiences are 'injected' with media messages
Illocutionary Act	A term in linguistics that describes a performative speech act, for example stating, asking, commanding, requesting
Informationalization of War	The increasing reliance of warfare on information and communication technologies
Internet	An international computer network
\Limited Effects	The theory that media messages have a limited effect on their audience, but that other factors may also have an influence
Media Effects	The theory that the media messages have an effect on their audience
Militarization of Cyberspace	The increasing assertion of military authority over the Internet
Military-Industrial Complex	A country's military establishment and the industries that produce arms and other military equipment
Pentagon	The headquarters of the U.S. Department of Defense
Perlocutionary Act	A term in linguistics that describes a persuasive speech act that has psychological consequences
Policy Window	An opportunity for attention to be given to a specific issue, which opens either due to a change in the political stream, or when a new problem comes to the attention of officials
Referent Object	The object or a idea to which a security threat is directed
Securitization	A successful speech act through which a variety of issues are framed by specific actors under certain conditions as issues of security
Securitizing Actor	A person who is able to perform a security speech act
Security Professional	A professional who works for the military, an intelligence agency, or law enforcement
Speech Act	A term in linguistics that describes an utterance that can be persuasive or performative
Telecommunications	Communication over a distance via cable, telegraph, telephone, or broadcasting

Threat Subject — The character of the threat posed to the referent object, or the form it takes

TiVo — A digital video recorder (DVR) developed and marketed by TiVo, Inc. and introduced in 1999.

World Wide Web — A system of hyperlinked webpages

Chapter 1.

Introduction

In the Summer of 2011, a United Nations report declared that access to the Internet should be considered a fundamental human right (La Rue, 2011), while the Pentagon declared that computer-based attacks, or ‘cyberattacks’ could be considered ‘acts of war’, potentially meriting a full military response (Gorman and Barnes, 2011). These statements illustrate the acknowledgement of the now paramount importance attributed by world leaders to the Internet, however they are indicative of very different concerns. The Pentagon’s announcement came in the same week as search engine giant Google's announcement that its digital systems had come under attack for the second time in as many years; an attack which seemed to have originated in China (Fiveash, 2011). Conversely the UN’s statement seems to have been prompted by the role the Internet played in the Arab Spring uprisings and the efforts on the part of Egyptian, Libyan, and Tunisian governments to control or even deny access to this valuable resource. The UN had responded by condemning the blocking of Internet access to quell political unrest (La Rue, 2011).

Concern with the centrality and integration of networked computing into all areas of society has received most scrutiny in the United States of America, which has spent the last two decades developing a detailed cybersecurity strategy, and is therefore a leader for most other countries in the development of cybersecurity policy. Its concerns have largely focused on two imperatives: the need for secure systems and the importance of freedom of access. Security and freedom are usually framed as opposites, with the former often being attained at the expense of the latter (Bigo and Tsoukala, 2008; Chandler, 2008). Political and economic debates within this frame tend to divide along lines of power; the military, intelligence community, and some members of government have been pressing for greater regulation and control of Internet-based communications, arguing that the security of the nation depends upon a secure Internet.

A burgeoning cybersecurity industry, spawned by the military-industrial complex, is busily developing solutions for every vulnerability, and marketing to government, industry, and individuals alike. And on the other side, civil rights groups including the Electronic Frontier Foundation, American Civil Liberties Union, and the Electronic Privacy Information Centre have raised concerns about the implication of these developments on civil liberties, and the need for balanced responses.

This duality of control and freedom lies at the heart of debates over regulation of the Internet, leading to an often complex framing strategy of Internet-related incidents. For example, during his 2008 presidential campaign, President Obama declared the U.S. information infrastructure a ‘strategic asset,’ a move which positioned the Internet as a significant issue for the military and illustrated the increasing militarization or ‘securitization’ of the Internet (Clarke and Knake, 2010, p. 116). Conversely in 2010, during the first wave of Chinese cyberattacks on the digital infrastructure of Google—and up to thirty-three other major U.S. companies—rather than frame the attacks exclusively as an issue of national security, the Obama administration took the opportunity to challenge China on its censorship policies, making Internet freedom “a central human rights issue” (Cha and Nakashima 2010, para. 8). Hillary Clinton’s speech on Internet freedom the following week proclaimed that “these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights... technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights” (2010, para. 9). The incident provided the opportunity for the U.S. to challenge, in the name of freedom and democracy, the absolute control that China and other states attempt to hold over their nation’s Internet. However the security measures being proposed domestically as a security response to the Chinese attacks promoted exactly this kind of control, and the risks to civil liberties that this entails.

Framing

These incidents illustrate the importance of 'framing' in the legitimizing of various responses. As Robert Entman explains, “[t]o frame is to *select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as* *to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation* for the item described" (1993, p. 52, emphasis in original). The same situation can be interpreted in many ways, prompting different responses and solutions, however the framework of national security creates an imperative to reduce risks at almost any cost, due to the potentially high cost if these threats are realized. Therefore the framing of Internet-based risks as posing a threat to national security legitimizes responses that increase control and surveillance as a way of minimizing risk, while at the same time reducing privacy and freedom of speech. The implementation of more restrictive security measures that result in a reduction in the privacy of a nation's citizenry and an increase in control for security professionals may be seen less as an unfortunate by-product and more as a favourable consequence when viewed through the lens of national security and political economy. As the Second World War and the Cold War have shown, efforts to combat credible threats to national security require the support of a burgeoning and lucrative security industry.

This thesis will look at the process through which vulnerabilities in the infrastructure, code, and use of the Internet are framed as national security issues, and how certain threat frames gain enough salience to be acted upon. It will assess competing frames that would push policy in a different direction, and the facilitating conditions that promote the acceptance of the national security frame. A combination of two theoretical frameworks will be used to examine this process; the first is from International Security Studies (ISS) and provides insights into the actors, power relations, and rhetoric of national security. The Copenhagen School of ISS has attempted to theorize the process of framing risks as issues of national security through its *securitization theory*, however it lacks the practical exploration of how security arguments reach their audience—insight that can be provided by framing research in Communications Studies as this framing process often happens in the media. By combining these two approaches this thesis seeks to bring further clarity and insight to the study of *cybersecuritization*.

Securitization is defined as a successful speech act through which a variety of issues are framed by specific actors under certain conditions as issues of security (Buzan and Hansen, 2009). A 'referent object'—in this case the state—is said to be threatened in its very existence, therefore necessitating urgent action (Buzan et al, 1998). This provides the justification for 'securitizing actors' to respond with countermeasures that may be disproportionate to the threat, and in the case of cybersecurity, may infringe upon civil liberties. Securitization takes a constructivist standpoint, seeking to broaden the concept of security beyond the traditional bounds of nation-state and military conflicts by examining discourses of insecurity or “representations of danger,” how they work, and what they do (Weldes et al, 1999, p. 10). This approach allows the researcher to denaturalize the common sense by subjecting it to scrutiny. By having the ability to define ‘reality,’ the dominant representations of insecurity are not critically engaged with; they are seen as objective truths, rather than “interested constructions” (ibid, p. 17). Constructivist approaches to security studies are particularly useful for examining cybersecurity as computer-based threats are often non-traditional, non-state, and non-military, and therefore fall outside the realm of traditional security studies. Such an approach also provides a framework for examining the vested interests behind a claim of security for new threats such as those in the cyber-realm, denaturalizing “the putatively given agents, such as states and other communities… the relations given among subjects… [and] the insecurities faced by those subjects as apparently objective threats” (ibid, p. 20).

However securitization theory is underdeveloped in a number of ways, most obviously with respect to the role of the audience. The audience is central to a securitization because, as Ciaran O'Reilly notes, in national security arguments, “the referent object and the audience are often one and the same” (2008, p. 68); those who are the target of the securitization are also often those who are threatened. Therefore the acceptance of a securitization is contingent on an argument that resonates strongly with the target audience. However the theory fails to develop an account of which audiences are targeted, how a security speech act reaches its audience in a practical sense, and when or why the securitizing move is accepted (Dunn Cavelty, 2008; Balzacq, 2005; Vultee, 2011). It is here that communications research into media effects can be used to develop the theory further, as it provides a long history of research examining how those in positions of power transmit their argumentative practices, and how and when these frames are accepted by an audience (Entman, 1993; Pan and Kosiki, 1993; Fairclough, 1989). While some Copenhagen School scholars have referenced the role of the media in the securitizing process, it has not been fully explored; meanwhile scholars of communications have long argued for the “centrality of media accounts in forming and shaping public opinions of distant events” (Vultee, 2011, p. 77; see also Lasswell, 1948; Katz and Lazarsfeld, 1955; Herman and Chomsky, 1988). Similarly, securitization can be used to develop a more reflexive understanding of media effects, by exploring the *facilitating conditions* which increase the likelihood of a frame’s success rather than looking at the speech act in isolation, and by looking at the media as an audience itself. The two approaches are therefore quite complementary, as can be demonstrated with a comparison of their central questions. Securitization seeks to assess who is able to securitize, who or what is threatened, the results of this securitization, and under what conditions this is able to occur (Buzan et al, 1998, p. 32). Similarly, media effects scholar Harold Lasswell asks ‘who says what to whom, through what channel and to what effect?’ (1948).

Several scholars have recently applied media effects insights to securitization in order to develop a more accurate understanding of how widespread support was garnered for military action in Iraq (O’Reilly, 2008), or how questions of immigration are framed as issues of terrorism (Vultee, 2011). While scholars have also significantly developed the centrality of the audience in securitization theory (Stritzel, 2007; Balzacq, 2005; MacDonald, 2008), and Myriam Dunn Cavelty has done so specifically with respect to cybersecurity (2008), there is currently a gap in the literature wherein a media effects approach could be applied to the securitization of cybersecurity. Cybersecurity, more than most other points of national vulnerability, is an ideal case study as it relies almost completely on hypothetical future events, which is a central tenet of securitization (Buzan et al, 1998, p. 32). Whereas the potential terrorist connections of immigrants, or the need to take military action in Iraq rely on the invocation of the 9/11 attacks and the threat of a repeat occurrence, there is no similar threat to point to in cybersecurity. References are made in cybersecurity literature to a range of past national security threats, from 9/11 to Pearl Harbour to nuclear war, but none of these examples clearly illustrate how a cyberattack might occur, what impact it would have, and what exactly people should fear. In the absence of a concrete example of the destructive power of a cyberattack, the persuasive strength of the framework, the position of the securitizing actor who performs the speech act, and the transmission of the message through mass media must be wholly relied upon to produce the desired effect in the audience.

Therefore an analysis of securitization as a theory of media effects as applied to cybersecurity would be an important contribution to the field.

Cyberspace

The following chapters will map the development of the 'cybersecurity' sector in the United States, wherein 'cyberspace' is constructed as both insecure and integral to the proper functioning of society, thus necessitating urgent action to combat threats. The definition of the term ‘cybersecurity’ will be developed throughout this thesis; however an initial working definition can be drawn from *S. 3480*, the *Protecting Cyberspace as a National Asset Act* of 2010. This document defines cybersecurity as involving the protection or defense of cyberspace, which encompasses “the interdependent network of information infrastructure, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries” (2010, p. 3). The popular understanding of cyberspace and cybersecurity usually refers only to the Internet, however it is important to bear in mind the wider telecommunications networks that support and are connected to the Internet, as well as the independent networks and intranets used by critical infrastructure.

Cyber-Threats

The securitization of cyberspace is a fairly recent phenomenon; only since the early 1990s has ‘cybersecurity’ developed as a concern, rather than simply ‘computer security’. This is because the network we know as ‘the Internet’ today was not developed with security in mind. As a military project, the security of ARPANET was based on the fact that it was a closed system with a small number of trusted users. Even after the military relinquished control and networked computing was commercially developed into the World Wide Web that we use today, there was no concept it would eventually be used by a seemingly unlimited number of largely anonymous users for financial transactions, the transmission of sensitive personal information, government communications, or increasing the efficiency of utility usage in homes. Internet legal scholar Jonathan Zittrain explores the way in which this openness has allowed for innovation, but has also posed problems for security in his book *The Future of the Internet*. He says of the Internet and the PC,

> [b]oth platforms were released unfinished, relying on their users to figure out what to do with them—and to deal with problems as they arose. This kind of openness isn't found in our cars, fridges, or TiVos. Compared to the rest of the technologies we use each day, it's completely anomalous, even absurd... We wouldn't want our cars, fridges, or TiVos to be altered by unknown outsiders at the touch of a button—and yet this remains the prevailing way that we load new software on our PCs. (Zittrain, 2008, p. Ix-x)

Today the majority of Internet-based communications in the U.S. travel over the same 'backbone' of fibreoptic cables that are owned and maintained by six commercial service providers: Verizon, AT&T, Qwest, Sprint, Level 3, and Global Crossing, causing concern about vulnerability to attack for two major reasons. Firstly, critical infrastructure—including information systems and telecommunication, energy and utilities, transport, and finance—is becoming increasingly dependent on networked computing, which includes some level connection to the Internet. By connecting critical infrastructure to these public providers, facilities could become vulnerable to attack, as they could be hacked into by outsiders and damaged. Fears about threats to critical infrastructure have been the main focus of state concern over cybersecurity for decades, though the validity of such concern is questionable—'networked' does not necessarily mean 'connected to the Internet,' a misunderstanding that fear-mongerers seek to exploit, as will be shown.

A second area of concern is that non-classified military, government, and intelligence communications, by and large, travel across these same commercial networks and therefore an 'attack' on a commercial network could affect the ability of these organizations to communicate. The Department of Defense's classified network, SIPRNET, uses a separate backbone router system, but the unclassified NIPRNET relies on access to the Internet. Similarly, most military-use hardware (computers, printers, scanners, webcams, etc) and software (for years Windows was the most popular operating system, despite the greater security offered by a more customizable OS like Linux) is bought 'off the shelf,' meaning that the machines and even the code that they run on come from all over the world (Clarke and Knake, 2010, p. 86). The lack of control and oversight in the production process has caused concern in military circles, where the fear is that vulnerabilities could be introduced, unintentionally or otherwise (Clarke and Knake, 2010; Clark and Levin, 2009). It has been suggested that software could house built-in ‘logic bombs,’ ready to go off on-command and shut down websites, communications networks, banking systems, and defense systems (Clarke and Knake, 2010). Alternatively viruses and trojan horses, unwittingly downloaded by hapless users, could spread rapidly through a network, building backdoors into systems and allowing for espionage or the theft of intellectual property (ibid). Because of this interconnectivity, national security is dependent not only on the military, but also on the behaviour of private industry and individual citizens. This dynamic has facilitated a push towards greater control of networks, and a need to convince individuals of the national security imperative online.

Civil Liberties

Given its by-design insecurity, this thesis does not question the fact that the Internet could be (and should be) more secure. However the implications of attaching the national security label to cyberspace legitimizes actions by government actors which necessarily restrict the freedoms of the populace. As Didier Bigo and Anastassia Tsoukala argue, security is mainly about sacrifice: of people, through determinations of who needs to survive, and of values, as violence and coercion are legitimized as an inevitable side effect of security (2008, p. 2). In cybersecurity discussions emphasis is often placed on the attribution of attacks—a difficult task in the anonymous realm of cyberspace—and their prevention through the monitoring of network traffic using deep packet inspection (Clarke and Knake, 2010; McConnell, 2010). A steady push has been made towards the reduction of anonymity online since the 1990s, when the government tried to mandate encryption technology known as the ‘Clipper Chip’. This chip would allow communications to be encrypted, thus providing privacy, but the government would hold a decryption key, in case this privacy was used to conduct terrorist activity (Saco, 1999). Unsurprisingly this idea was rejected by citizens and businesses alike. However the imperative to remove anonymity has only grown more urgent as networked communications have become more integrated into society. The National Security Agency’s warrantless wiretapping program—begun in secret but publicly justified by the national security imperative—is an example of the belief among security professionals of the necessity of surveillance online, regardless of the impact on law-abiding citizens (Kravets, 2011).

A less popular suggestion is the ‘lockdown’ method highlighted by Zittrain, wherein networks and the connected critical infrastructures are more strictly regulated by government—a distasteful suggestion for private industry. The recently discussed *Cybersecurity Act* went so far as to propose that the President be given an Internet ‘kill swtich,’ or the authority to tell any service provider, website, or infrastructure owner to shut off connection to the Internet in the event of a ‘disruption’ in cyberspace (Sanchez, 2009). The possibilities for misuse were obvious enough that the Bill was quickly rejected. However the scheme resurfaced the following year in the Protecting Cyberspace as a National Asset Act (2010). The degree of invasiveness and restriction afforded by these surveillance and control measures will vary depending on which security actor’s argument carries the most weight. Therefore in analyzing the impact of the dominant argument, this thesis will question whether cyberspace will be preserved as an open, global commons of information, or whether we will see increasing digital controls, regulation, and surveillance (Deibert, 2003; Deibert et. al, 2010; Saco, 1999). Unfortunately for civil rights advocates, the political and economic interests of security industries and the military are very much in line (Edwards, 1996; Singer, 2003; Smythe, 1986).

Chapter Outline

The first chapter will outline the benefits that a constructivist perspective brings to the analysis of cybersecurity, and will then outline *securitization theory*, the social constructivist framework of the Copenhagen School. It will highlight the strengths and weaknesses of this approach, and insights that other scholars—particularly Myriam Dunn Cavelty (2008)—have brought to the theory which develop it further. The main critique of securitization theory will be that it focuses on the 'perlocutionary' (persuasive) or 'illocutionary' (performative) elements of the speech act—the linguistic construction of a declaration of insecurity—while it is less clear about the circumstances in which this speech act occurs, how these circumstances facilitate its acceptance, and the role that the audience plays in this process. Using Dunn Cavelty's insights as well as the incorporation of media effects research, this chapter will suggest that the media has a central role to play in the construction, dissemination, and acceptance of the national security frame. At the end of the chapter some alternative frames will be outlined, and it will be suggested that the media can promote the acceptance of security frames, or question them and support the acceptance of alternative frames.

In order to avoid a "hypodermic needle" approach to media effects which ignores audience agency and individual differences, it is important to bear in mind Tiery Balzacq's contention that securitizations are accepted by an audience "based on what it knows about the world" (in Vultee, 2011, p.78). This consideration of context is essential; actors cannot simply 'speak security' about any topic and have an effect. However given the right context, acceptance of a securitizing move is more likely. Therefore the second chapter will review the development of the concept of cybersecurity in order to highlight the *facilitating conditions* that make networked computing uniquely suited to securitization and militarization, and the reasons that computer security became a concern of national security at the time that it did. The centrality of networked computing in today's society has prompted concerns over the vulnerabilities this could introduce to critical infrastructure, and a variety of recent incidents have suggested that this fear is not unfounded. This has resulted in an assessment of cybersecurity using a national security framework rather than one of technical computer security. However this shift did not occur suddenly and independently; there is a long historical relationship between networked computing and the military. Since the First World War, societal, geopolitical, and technological shifts have changed the way that wars are fought, necessitating the use of more and more advanced technology due to the need for more accurate weaponry. These shifts in warfare strategy have been variously referred to as total vs. limited war, conventional vs. counterinsurgency, symmetrical vs. asymmetrical, modern vs. postmodern, and the revolution in military affairs (Whyte, 2010; see also Gray, 1997; and Berkowitz, 2003). While their emphases differ, these labels all reference changes in the way wars are fought, the blurring of the apparent distinction between civilian and military affairs, and the expansion of the concept of national security beyond the scope of traditional warfare to combat adversaries as wide-ranging as poverty, drugs, and terror. It was in this context of the *informationalization of war* that the military project

ARPANET was created. Similarly the expansion of the military mandate has allowed for the *militarization of cyberspace*, as information communication technologies have become a focal point not only for the military-industrial complex—sometimes referred to as the cyber-industrial complex—but also for the various military departments seeking to justify their continued existence and influence following the end of the Cold War and the resulting threat deficit. In looking at this history it is possible to identify the *facilitating conditions* which allow for cybersecurity to be brought to the attention of government officials, providing a ‘policy window’ through which the problem can be moved into the political agenda.

In the third chapter a combination of quantitative and qualitative methods will be used to gather and analyze data illustrating the media framing of cybersecurity. Using content analysis, a set of keywords that are representative of cybersecurity discourse will be used to locate news articles in the U.S. media publications with the widest circulation during the period spanning the last three administrations. Cybersecurity was accorded a prominent role in national security strategy during Bill Clinton’s presidency, although its origins can be traced back much further (Dunn Cavelty, 2008, p. 66). This thesis will look at the development of a cybersecurity agenda during the Clinton, Bush, and part of the Obama administrations. The data set will then be assessed using a framing analysis that draws on insights from Robert Entman, as well as Norman Fairclough's Critical Language Study (1984). The combination of quantitative and qualitative methods not only allows for the identification of trends over time, indicating growing public awareness of cybersecurity issues and the periods during which they received most attention, but also shows how the discourse has shifted around these issues, how other events may have affected who and what is perceived as a threat, and whether the media endorses or questions the securitizing frame.

The fourth chapter will present the analysis of securitization as a media frame of cybersecurity. Within securitization theory, the media can be seen as both an audience and as ‘functional actors,’ or actors who influence the dynamics of the security field without being the ones to actually perform the security speech act. By choosing either to promote audience awareness of the security speech act by using the frames of the securitizing actors and publishing their opinions, or choosing to promote alternative and conflicting frameworks, the media can influence whether a securitizing move is likely to reach a wider audience. To this end, this analysis will show how the popular understanding of the term ‘cybersecurity’ has developed over the last three administrations, highlighting the competing frameworks that are present in discussions of cybersecurity, and explaining how they can influence the meaning attributed to events. Whether or not events are understood to be issues of cybersecurity will affect whether they function as ‘focusing events,’ i.e. events which allow a condition to be seen as a problem necessitating action, and thereby giving certain actors the opportunity to gain attention for this problem area on the political agenda (Dunn Cavelty, 2008). The suggestion is not that media framing necessarily shapes policy, but rather that there is a connection between the agenda-setting function of news media, and the ability of parallel discourses in policy to become predominant, operationalizing responses to threats which increase government control over the Internet.

The final chapter will take a detailed look at a case study highlighted by the data analyzed in the previous chapter and which exemplifies security professionals' use of the media to promote their preferred framing of cybersecurity incidents. Using a second data set, the chapter will analyze the framing of the 2010 cyberattack on Google and up to thirty-four other U.S. organizations which was attributed to China. This is an excellent example of the importance of media framing to the interpretation of cybersecurity incidents, and the ability of the media to question this framing. The Google and China incident can be seen as a flashpoint in the development of securitizing rhetoric around cybersecurity. It is clear that the targeting of the U.S. technology industry was not an unusual occurrence, and that U.S. industry as well as government and defense had been having problems with Chinese hackers for years. What makes this incident so significant is the fact that, not only do the combined efforts of Google and the U.S. government clearly influence the framing of the cyberattack so that it is seen as a major security incident, but they successfully reframe the debate over the sacrifice of civil liberties in the name of security, portraying increased government regulation and control as necessary for Internet freedom.

This thesis will address the following questions: how does computer security become framed as a concern of national security? How is it placed on the political agenda? What are the implications of addressing cybersecurity through a national security framework? How does the construction of the threat change over time? What consideration, if any, is given to civil liberties? And finally, can the media influence the acceptance of these frameworks, and thus promote the securitization process, or even promote alternative frameworks and encourage dialogue and dissensus?

Chapter 2.

Theories of Securitization as Media Effects

> No other concept in international relations packs the metaphysical punch, nor commands the disciplinary power of ‘security.’ In its name peoples have alienated their fears, rights and powers to gods, emperors, and most recently, sovereign states, all to protect themselves from the vicissitudes of nature – as well as from other gods, emperors, and sovereign states. In its name weapons of mass destruction have been developed which transfigured national interest into a security dilemma based on a suicide pact. And, less often noted in [International Relations], in its name billions have been made and millions killed while scientific knowledge has been furthered and intellectual dissent muted. (Der Derian in Nissenbaum, 2005, p. 69)

As this quote from James Der Derian points out, the ability to ‘speak security’ can have an enormous impact on the willingness of a population to tolerate violations of its civil liberties and more, in order to ensure its safety. This understanding that safety comes at a price suggests that security is mainly about sacrifice: of people, through determinations of who needs to survive, and of values, as violence and coercion are legitimized as an inevitable side effect of security (Bigo and Tsoukala, 2008, p. 2). This state of affairs has been exacerbated by the September 11, 2001 terrorist attacks, which promote a new conceptualization of security in which everyone is a potential threat and everyone is therefore suspect, an attitude that neatly continues from anti-Communist fears and initiatives (Lyon, 2003, p. 7). As Jennifer Chandler points out, “[s]ince terrorism (particularly suicide terrorism) is not easily deterred by punishment after the fact, the pressure to detect and preempt terrorist plots is strong. Increased surveillance is therefore a predictable response to a dramatic terrorist attack” (2008, p. 125). The increase in the ability to process and analyze huge amounts of digital information that is made possible by computerization and the level of incorporation of digital technologies into everyday life, provide opportunities for surveillance like never before (Haggerty and Ericson, 2006). This drive towards increased surveillance and control is also a result of arguments that our national digital infrastructure is vulnerable to attack, and therefore so are the many critical infrastructure systems that depend on it—including energy and utilities, transport, and finance (Clarke and Knake, 2010; Clark and Levin, 2009; Deibert, 2003; Nissenbaum, 2005).

The process through which officials are able to ‘speak security’ and thereby designate an issue as a threat is explored by the Copenhagen School’s theory of ‘securitization’. This provides a useful starting point to explore the way in which networked computing is characterized as threatened or threatening. Drawing from speech act theory, the Copenhagen School posits that the securitization process begins with a ‘speech act’ or a performative utterance which can bring about a condition by pronouncing it, similar to the idea of a pronouncement of marriage (Austin, 1975). Securitization also has some clear similarities to framing, in that the issue is linguistically constructed in a specific way to encourage a desired effect. However beyond the speech act itself, how is an issue brought to the attention of both policymakers and the public, and placed on the security agenda? The Copenhagen School itself acknowledges that just speaking security is not in itself enough, and there are other ‘facilitating conditions’ which need to be present in order for a securitization attempt to be successful (Buzan et al., 1998). Most notably, the socio-political position of the ‘securitizing actor’ or the person who performs the speech act must be such that he or she is in a position of authority and is an accepted voice of security. However as Myriam Dunn Cavelty (2008) has explored in an important critique and development of securitization theory, the process through which an actor comes to speak security, and what happens after, eventually resulting in the acceptance of the speech act, is far more complicated and reflexive than the Copenhagen School’s framework acknowledges. Her critique will be outlined here in order to explore securitization as a more comprehensive framework, however it is still somewhat lacking as it does not explain how exactly the security speech act reaches its audience in order to be accepted and responded to.

This is where communications research into media effects can be useful, as it has highlighted the framing and agenda-setting functions of media, and the complex ways in which messages are encoded, decoded, and responded to. Gaye Tuchman suggests that “news imparts to occurrences their public character as it transforms mere happenings into publicly discussable events” (1978, p.3). Fred Vultee echoes these sentiments in his exploration of securitization as a theory of media effects, wherein he notes, “[m]edia frames are the lens through which the public sees an issue... either as a routine matter best dealt with through the normal workings of law enforcement and politics or as a crisis that requires extreme measures for indefinite periods” (2007, p. 3). While this may not produce the desired effect of the frame as there is no guarantee that an audience will accept what it is told by the media, research suggests that under the right circumstances, the media can have an agenda-setting function, and can influence opinion formation (Robinson, 2001; Pan and Kosiki, 1993; Entman, 1993). Harold Lasswell’s (1948) question, posed over eighty years ago, of ‘who says what to whom, in what channel, and to what effect’ set the tone of communications research for a generation, and bears strong similarities to the central question of securitization theory, which asks who is able to securitize, who or what is threatened, what are the results of this securitization, and under what conditions is this able to occur (Buzan et al., 1998, p. 32). Therefore the insights of communications theorists that have built upon, questioned, and developed the work of Lasswell and other scholars of media effects can provide much-needed clarity on how security speech acts are transmitted to an audience, and what conditions are necessary for their acceptance.

This analysis will begin by looking at the rhetorical power of the concept of security and the ways in which it can be successfully applied to networked computing or ‘cybersecurity’, before turning to the discursive process of securitization to show how the threat is constructed, and finally looking to research into media effects to establish the role of the media in the dissemination of these ideas. It will argue that research shows some degree of influence by the media on public opinion, although this is mediated by multiple external factors as well as personal variables. It will also suggest that the institutional conventions of the media predispose it to supporting a securitization attempt; however this does not have to be the case. There may be some situations in which it is possible for the media to play a more active role in deciding the success of a securitizing move. The little research that exists on securitization and the media has thus far focused on the effect of the media on audiences, thereby assuming the acquiescence of the media in the securitization process. This chapter questions that assumption, and seeks to develop a fuller understanding of the role of the media in securitization, and in cyber-securitization specifically.

What is ‘Security’?

In security studies, ‘security’ is generally understood to involve the state and its experience of threats (Weldes et al., 1999, p. 9). Drawing on Arnold Wolfers’ definition of national security as “the absence of threats to a society’s core values”, Eriksson and Giacomello suggest that, “[i]f modern, economically developed countries are increasingly becoming ‘information societies’, then, following Wolfers’ argument, threats to information can be seen as threats to the core of these societies” (2007, p. 2). However, what these core values are and how they should be protected is understood differently through different theoretical perspectives. The three main perspectives in security studies are realism, liberalism, and constructivism, and they bring different elements to the study of security. Eriksson and Giacomello argue that constructivism, which is the basis for securitization theory, is the best fit for examining the discursive process through which cyberspace is framed as a concern of national security. *Realism* takes the state as its primary unit of analysis, and therefore there is little room in this interpretation for non-state actors to exercise power. Eriksson and Giacomello suggest that “[r]ealists might consider IT-related security threats to be largely an economic issue, not necessarily affecting the security of states and not in themselves security threats” (ibid, p. 12). If such threats were to be acknowledged, it would be through an information warfare framework, as a new technological or psychological component in a traditional conflict (ibid). *Liberalism* takes a much broader perspective, emphasizing the plurality of international actors and the significance of non-state actors, as well as the importance of domestic political factors on the behaviour of states (ibid, p. 13). This broader view is more suited to an analysis of cybersecurity as attacks are not often militarily-based, attribution is difficult due to the remote nature of the attacks and the ease of anonymization, and cyberthreats involve a range of trans-national actors. However liberalism tends to see the costs of the interdependence promoted by ICTs in economic terms, and it tends to take an optimistic perspective on interdependence, rather than seeing it as increasing vulnerability and insecurity. While networked computing has created tremendous benefits, it is important to acknowledge that it has also brought vulnerabilities and can be misused (ibid, p. 14 and p. 17).

Constructivism emphasizes the interpretative nature of social reality and its distortion depending on that interpretation. As Eriksson and Giacomello explain,

> [a]t the most basic level, actors have a set of norms—beliefs about right and wrong. Norms shape identities—the separation of 'we' from 'them.' In turn, identities shape interests. Importantly and in contrast to rationalism, all of these elements are seen as inherently dynamic. If interests change, it is because there is an underlying shift in identities and norms. (ibid, p. 18)

In contrast to realism and liberalism, "[c]onstructivism... does not take a general stance as to what can or cannot be framed as a security threat and how such threats can be dealt with" (ibid, p. 19). It focuses instead on how disparate issues *become* threats. This means that the widest possible range of security threats can be addressed. In looking at the construction or framing of reality, constructivism makes clear the choices that result in the characterizing of issues in certain ways. Copenhagen School scholars Buzan et al. assert that "[a]ctors can choose to handle a major challenge in other ways and thus not securitize it. The use of a specific conceptualization is always a choice—it is politics, it is not possible to decide by investigating the threat scientifically" (1998, p. 32).

Acknowledging that threats to security are constructed does not mean that they are fictional. This becomes clear by looking at security and the related concepts of risk and vulnerability. Risk refers to imagined futures; as Ulrich Beck has explained, "risks are not 'real', they are 'becoming-real'"—they are not real until they actually occur, at which point they become a catastrophe (in Van Loon, 2002, p. 2). Similarly Buzan et al. explain that discussions of security are "about the future, about alternative futures—always hypothetical—and about counterfactuals: What will happen if we do not take 'security action'... and what will happen if we do?" (1998, p. 32). Anthony Giddens traces the origin of the word 'risk' into banking and investment, where it "came to refer to a wide range of... situations of uncertainty" (2002, p. 22). There is no concrete way to predict future 'reality,' only possible constructions of future realities. While risk implies an assessment or evaluation of a situation to ascertain the likelihood of a set of outcomes, this assessment is just as prone to subjective influence as an assessment of security threats. Security and risk are based upon the idea of vulnerability, which "refers to a system's *condition*- to its ability to anticipate, resist, cope with, and possibly recover from events that could reduce the system’s functional integrity” (Bijker, 2006, p. 57). Conversely risk—and security—differs in that it is “an outcome-oriented notion. It conceptualizes the *effects* of a possible, harmful event” (ibid). Vulnerability can therefore be understood as an objectively characterized weakness in the system, and whether this results in outcomes that are good or bad is down to the interpretation and contextualization of those weakness—how they are constructed or framed.

In this way, constructivism can be used to understand the relationship between vulnerability, risk, and security. As Bijker explains,

> [a] vulnerable system may yield certain risks, when it could produce damage, depending on the circumstances. A risk analysis can, vice versa, be helpful in assessing a system’s vulnerability: analysing the chances (and resulting damage) of subsystem or component failure may help to get to grips with at least the technical aspects of a system’s vulnerability. (ibid)

This is especially relevant to an assessment of threats to the security of the Internet, as its vulnerabilities can also be seen as its greatest strengths. While the openness and flexibility of the Internet make it vulnerable to manipulation and attack, these are also the qualities that make it most resilient and effective for independent coordinated action, and for innovation. Bijker highlights the importance of acknowledging this duality in risk assessment when he notes the necessity “to assess risks and benefits within one framework: risks cannot be evaluated without also evaluating the positive effects of the actions that generate them” (Bijker, 2006 p. 57).

Constructivism is also particularly useful when looking at issues of cybersecurity as threats to or through networked computing would not traditionally be seen as issues of *national* security. However if we understand ‘security’ as a constructed concept wherein it represents “the condition of being protected from danger, injury, attack (physical and non-physical), and other harms, and protection against threats of all kinds,” the ‘harm’ that can be caused will be dependent how security is constructed (Nissenbaum 2005, p. 64). Constructing a threat as causing national rather than technical harm legitimates a specific type of response. As Helen Nissenbaum illustrates, in a technical computer security framing, protection from the threat of harm focuses on attacks which threaten the availability, integrity, or confidentiality of a system, an imperative which is arguably consumer or private interest-driven rather than suggesting a moral imperative (ibid, p. 64-65). As a result, solutions seek to fortify individual nodes on the network in order to strengthen protections before attacks occur, rather than attempting to identify would-be attackers (ibid, p. 71). However imbuing computer security with the moral force of national security promotes different strategies of protection from harm. Such a response seeks to stop an imminent attack before it occurs by making everyone suspect, and therefore promoting increased centralized surveillance (ibid).

Cybersecurity incidents are also often framed as national security issues even though they seem to be more accurately described as instances of computer-based crime. For example the often-cited computer-based attacks perpetrated against Estonia in 2007, and Georgia in 2008 involve strong elements of 'cybercrime' but are popularly seen to be some of the first examples of 'cyberwar' (Clarke and Knake, 2010). Micheal Van Eeten and Johannes Bauer explain that these incidents "combine criminal resources and terrorist purposes" as the attacks targeted the infrastructure of a nation-state, but used computer resources from Russian criminal organizations. In addition, no nation claimed responsibility and the attacks could not be clearly attributed (2009, p. 229-230). The choice of a national security frame rather than one of law enforcement is significant to the construction of these attacks because they produce "very different and conflicting policies, both in terms of goals as well as means" (ibid). The law enforcement framework acknowledges that "it is economically rational to tolerate certain level of insecurity [sic]" and "[a]ll markets are afflicted with a certain level of crime", however "[t]he costs of higher security have to be weighed against the benefits" (ibid), which bears similarities to Bijker's assessment of the duality of vulnerability in risk assessment. By contrast, the national security framework does not look at actual damage, but rather potential damage—'potential' being understood in terms of worst-case scenarios. As the worst-case scenarios are potentially very severe, the logical response is to do everything possible to prevent such events from happening. As a result, Van Eeten and Bauer explain that,

> rather than interventions based on actual costs and benefits of (in)security for societal actors, the interventions would be driven by the potential costs to society of attacks that have not yet occurred. The word 'benefits' is missing from the last part of that sentence because they

> rarely seem to play a role in national security when considering policy options. (ibid)

This focus on potential futures is further complicated due to the reliance in the security field on 'experts' who are not always held accountable. As Didier Bigo notes, there is a “lack of precision required for threats identified by the professionals who know some ‘secrets.’ Amateurs always need to ‘prove’ their claims, whereas professionals, whether public or private, international, national, or local, corporate or public, can evoke without demonstrating” (2002, p. 74). Lene Hansen and Helen Nissenbaum argue that while the reliance on technical, expert discourse is not unique to cybersecurity, “[technifications] have been able to take on a more privileged position than in any other security sector” (2009, p.1168) as the field of computer security often requires knowledge that is not available to the general public. This is important because—as speech acts that are similar to securitization—the effect of 'technifications' is that “they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda, that technology serves” (ibid, p. 1167). Therefore the simultaneous use of both securitization and technification in cybersecurity discourse is significant because they “work to prevent it from being politicized in that it is precisely through rational, technical discourse that securitization may 'hide' its own political roots” (ibid, p. 1168).

It is therefore important to interrogate a construction of computer security as having national security impacts. Given the reliance of so many areas of society on the proper functioning of the Internet, as well as the apparent vulnerabilities that connectivity introduces to critical infrastructures, and the centrality of networked communication to the military and to government, the security of the Internet can be argued to be of national importance. However, it is clear that constructing a computer security issue as relevant to national security necessitates certain responses. This invocation of security and its effects is the object of study of Barry Buzan, Ole Waever, and Jaap de Wilde of the Copenhagen School of International Security Studies. Their theory of ‘securitization,’ outlined in their 1998 book, *Securitization: A New Framework of Analysis*, will be the starting point for the framework of analysis developed in the rest of this chapter.

Securitization Theory

Situated between security studies, speech act theory, and the Schmittian concept of state and security politics, the Copenhagen School's concept of security involves "national security discourse, which implies an emphasis on authority, the confronting—and construction—of threats and enemies, an ability to make decisions, and the adoption of emergency measures" (Hansen and Nissenbaum, 2009, p. 1158). Securitization can be seen as a part of threat politics, that Myriam Dunn Cavelty defines as "the political process by which threats are moved into and removed from the political agenda or which alters the face of threats on the political agenda" (2008, p. 24). In its focus on agenda setting, securitization can be seen as a type 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, p. 54). The type of frame used may provide completely different interpretation of events, and therefore suggest different solutions when compared to another frame. Threat frames, according to Dunn Cavelty, involve the development of interpretive schemata through which agents decide whether something counts as a threat or risk, how to respond, and who is responsible (2008, p. 30). According to this understanding, security is not an objective or subjective condition, but rather a concept that has a discursive and political force that 'securitizes' (Hansen and Nissenbaum, 2009, p. 1158).

The construction of a securitizing move involves a 'referent object', in this case the state, which is said to be threatened in its very existence, therefore necessitating urgent action (Buzan et al., 1998). This provides the justification for securitizing actors to respond outside normal political procedure with countermeasures that may be disproportionate to the threat, and may infringe upon civil liberties. According to the Copenhagen School, "[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" (Buzan et al., 1998, p. 21). In some cases, a securitizing move can even be expanded beyond a 'normal' level by exaggerating threats and promoting excessive countermeasures, a situation that Buzan terms a 'hypersecuritization' (2004, p.172). If a securitizing move 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. Therefore the central question of securitization theory asks who is able to securitize, which issues or ‘threat subjects’ are securitized, who or what is threatened (the referent object), the results of this securitization, and under what conditions this is able to occur (Buzan et. al, 1998, p. 32).

In focusing on the framing of insecurities, Buzan et. al are less concerned with providing an objective characterization of threats, vulnerabilities, and modes of defence, and more with providing a systematic account of the ways specific conditions, states-of-affairs, or events are posed by significant social actors as threats to security and come to be widely accepted as such. As Dunn Cavelty notes, this perspective essentially absolves the researcher from the task of judging whether or not a threat is ‘real’ (2008, p. 25). Without a clear understanding of the ‘reality’ of the threat, it is difficult to establish an accurate characterization of the threat subject, and the legitimacy of the securitization. But attempting to put forward an idea of objective ‘reality’ is also problematic, especially in an area as subjective as security. As Jennifer Chandler notes, security is not a limited value, and so we are likely to want more of it regardless of any objective characterization of the situation. However this can be problematic as obtaining security often involves giving up some of another value such as privacy (2008). Estimations of what level of insecurity can be tolerated, how much security to strive for and how much privacy to relinquish will be different for different people, dependant on various factors such as institutional or cultural influence. Yet even subjective estimations of the threat subject can be considered to be just as important as objective or ‘real’ estimations, as a response can be easily mobilized when there is a subjective understanding, whereas a lack of subjective response to a ‘real’ or objective threat could be more dangerous for a nation, as it creates a false sense of security and promotes behaviour that might otherwise be seen as unwise. Securitization theory holds that those with the power to speak security have the ability to define reality, and therefore the researcher must denaturalize the 'common sense' by viewing dominant representations of insecurity not as objective truths but rather “interested constructions” (Weldes et al., 1999, p. 17). This allows for the examination of the vested interests behind a claim of security for new threats such as those in the cyber-realm, questioning “the putatively given agents, such as states and other communities… the relations given among subjects… [and] the insecurities faced by those subjects as apparently objective threats" (ibid, p. 20).

The concept of securitization 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, p. 362). This idea is taken from speech act theory, developed by Austin (1975) and suggests that language is performative in that "expression is a social act involving a sender and a receiver who operate under arbitrary conventions or 'constitutive rules' that affect their behaviour" (Dunn Cavelty, 2008, p. 25). However as Fred Vultee points out, this conceptualization contains an unresolved contradiction: "How can the act of speaking security be performative if it relies on the consent of the audience?" (2011, p. 77). Buzan et al. qualify their speech act proposition by explaining that it is "not defined by uttering the word *security*. What is essential is first the designation of an existential threat requiring emergency action or special measures, and then the acceptance of that designation by a significant audience" (1998, p. 27; italics in original).

Despite acknowledging the central importance of the audience, this remains an underdeveloped aspect of securitization theory. Ole Waever himself has highlighted the conceptual flaw of the operationalization of audience acceptance, as "it remains largely unclear which audience has to accept what argument, to what degree, and for how long" (in Dunn Cavelty, 2008, p. 26). Further, the theory suggests that there are two 'facilitating conditions' which promote the acceptance of a securitizing move, but does not explore how these conditions aid the process. Insights from framing as a theory of media effects could therefore be helpful in exploring the way in which audiences come to accept a securitization. Vultee points out that the central question of securitization is very similar to Harold Lasswell's model of communication: "who says what to whom, through that channel, and to what effect" (1948). This model underlines the central influence of the media in the forming and shaping of public opinion, and its insights could therefore enhance our understanding of how the audience functions in securitization theory.

Securitization and Media Framing

The Copenhagen School's theory of securitization employs a broader understanding of 'security' than is allowed for by more traditional security studies scholars, and it can be applied to a wide range of fields—for example the environment or the economy as well as the nation-state—however the actors who are able to securitize in each of these areas are very different (Buzan et al., 1998, p. 22-23). When examining national, or state and militarily-oriented security, it is clear that security is to some degree institutionalized, and therefore certain actors are able to speak from a position of greater authority. Certain actors speak on behalf of the state and are also understood to act—theoretically—in the best interests of the populace. A social contractarian understands this dynamic as the voluntary giving up of a certain measure of an individual's freedom in exchange for the protection of a legitimate political authority, thus ensuring that "security is a primary obligation of the state since that is what individuals have contracted for in submitting to state authority" (Chandler, 2008, p. 126). Taking this understanding, political leaders, governments, the military, and various security professionals are already accepted voices of security.

According to Antonio Gramsci, political society or formal government apparatus work in conjunction with civil society (which includes the media, the church, universities etc) to develop "historically organic ideologies" (Gramsci 2005, p.376). The civil society institutions in this 'hegemonic bloc' produce "the complex of ideas, values, and ideologies which together form the 'common sense' of society and provide a bloc with 'an element of ... moral and intellectual order'" (Pozzolini, in Neubauer, 2011, p. 197). This conceptualization of society suggests that the media plays a central role as one of the spaces through which the "permanent persuaders" of the public could make themselves heard (ibid). Similarly Der Derian asserts that "[e]vents come wrapped in representations, bundled in ideology, edited by the media, distorted by official stories" (Der Derian, 2008, p.70). In their seminal text, *Securitization: A New Framework for Analysis*, Buzan et al. allow for the potential role of the media as a securitizing actor in some cases. This idea is not explored further, and given the institutionalization of national security, it is unlikely that the media would be able to securitize an issue by itself, as it does not speak from a position of authority on national security.

However this does not mean that the media is insignificant in the process of securitization. Fred Vultee suggests that the media is “the lens through which the public sees an issue” (2007, p. 3), which has major implications for the requirement of 'audience acceptance' in securitization. This is especially the case with a highly technical field such as computer security, due to media conventions that promote a reliance on expert opinions, as will be explored (Pan and Kosiki, 1993). As noted earlier by Bigo (2002) and Hansen and Nissenbaum (2009), cybersecurity is a field which is prone to technification due to the prominence of and reliance upon experts. As a result, “[t]he mobilization of technification within a logic of securitization is thus one that allows for a particular constitution of epistemic authority and political legitimacy” (Huysmans in Hansen and Nissenbaum, 2009, p. 1167). To add to this, Hansen and Nissenbaum also note the importance of the ability to manage public opinion of cybersecurity, as the public is understood to have a direct impact on the security of the nation through its own actions in cyberspace. Therefore securitizing actors seek to “mobilize 'normal' individuals' experiences in two ways: to secure the individual's partnership and compliance in protecting network security, and to make hypersecuritization scenarios more plausible by linking elements of the disaster scenario to experiences familiar from everyday life” (2009, p. 1165). These arguments thus suggest that the role of the media in the securitization of a technical field like computer security could be a pivotal one.

In spite of this, the role of the media in securitization, and especially with regards to cybersecurity, remains underexplored. Myriam Dunn Cavelty (2008) has expanded upon the theory significantly, however she does not pay much attention to the role of the media in promoting certain threat frames, or indeed how the frames are promoted at all outside of internal political processes. Little consideration is given to the role of any audience outside of policymakers and technocrats, despite the importance that these groups place on public representation. Helen Nissenbaum (2005) has also been successful in developing an understanding of the application of a discourse of national security to computer security, and her work with Lene Hansen (2009) has argued that securitization theory should be applied to this field—an application that Copenhagen School founders had previously dismissed (Buzan et al., 1998). They argue that the apparently disjointed sector of cybersecurity can be better understood when examined through a securitization framework, which makes clear the connections between a "wealth of referent objects, competing securitizing actors, and multiple threat constellations" (Hansen and Nissenbaum, 2009, p. 1157). In a 2005 paper, Nissenbaum also acknowledges that "[i]t is possible... that others in a society [besides military and government officials] might have achieved sufficient salience and persuasive capacity to construct the conception of threat necessary for securitization. One could imagine that trusted media sources... might accumulate this degree of salience" (p. 67). She notes the presence of a securitizing discourse in media sources, but does not go any further towards exploring the role of the media in a successful securitization, or the significance placed on the media by securitizing actors. Similarly Ralph Bendrath notes that the entertainment sector has capitalized on the popularity of what Dunn Cavelty (2007a) refers to as "cyber-doom" scenarios. He highlights the wealth of movies, popular fiction, and TV shows that take hacking, cyber-terrorism, and cyberwar as their subjects (Bendrath, 2003). Examples include classics from the 1980s like the movie *Wargames* and the novel *Neuromancer*, and more recent hits like TV series *24*, and movie *Die Hard 4.0*. Bendrath notes that "these works are not made only for entertainment. They produce certain visions of the future and of the threats and risks looming there" (ibid, p. 49). However he does not consider the parallel role that news media plays in this shaping or framing of reality, and of the public perception of risk.

There are a number of scholars who have identified this weakness in securitization theory, and they point to a wealth of literature on media effects and framing which could be used to enhance the understanding of the role of the media in securitization (Balzacq, 2005; Vultee, 2011; O'Reilly, 2008). In the Copenhagen School's terms, the media can be seen as a 'functional actor': an actor who is able to "affect the dynamics of a sector... [and] who significantly influences decisions in the field of security" (Buzan et al., 1998, p. 36). The media are able to exert this influence through a central aspect of securitization: the facilitating conditions through which an audience comes to accept a securitizing move. Buzan et al. explain that these conditions fall into two categories; firstly internal or linguistic-grammatical elements, and secondly external or contextual and social elements. The internal elements which consist of the identification of the existential threat to a referent object necessitating extreme measures in response. In Dunn Cavelty's terms, this involves viewing the frame as an *independent variable*, meaning that it is understood to be able to have an effect in its own right. This view highlights a number of problems within securitization theory which will be explored later, including the underdeveloped criteria of 'audience acceptance' and the equally vague and subjective idea of 'extraordinary measures' (2008). The second condition considering the external elements of a securitizing move approaches the frame as a *dependant variable* which is a product of the situation in which it is created. This necessitates an examination of the socio-structural or organizational factors that might influence the way key actors frame security issues, and suggests that institutions and their normative orders, values and bureaucratic subcultures can constrain the construction of reality (Dunn Cavelty, 2008, p. 31). For example Buzan et al. note that, with recurrent or persistent threats, the sense of urgency is often institutionalized, as in the military "where states have long endured threats of armed coercion or invasion and in response have built up standing bureaucracies, procedures, and military establishments to deal with those threats" (1998, p. 27-28). In what follows, the role of the media will be examined in framing as both an independent and a dependent variable, or as Fred Vultee terms it, framing as an effect *of* media and an effect *in* media (2011).

Linguistic-Grammatical Elements: An Effect **of** *media*

By looking at the frame as an independent variable and examining its effects, a number of weaknesses in the securitization model can be seen, specifically to do with the underdeveloped idea of 'audience acceptance', wherein it is unclear how and why an audience comes to accept the securitizing speech act. The equally vague idea of 'exceptional measures' is also problematic as the judgment of what is exceptional is quite subjective. Insights from communications research can be used to develop these elements. If Vultee is correct in characterizing media frames as "the lens through which the public sees an issue" (2007, p. 3) then the media may have a strong role in the question of whether or not an audience accepts a securitization, as it will likely be experienced through the media. As has been noted, news can transform occurrences into "publicly discussable events" (Tuchman 1978, p. 3), while the frameworks employed "narrow the political alternatives" (ibid, p. ix). Further to this, Tuchman highlights the agenda-setting function of news media, wherein "[t]hose topics given the most coverage by the news media are likely to be the topics audiences identify as the most pressing issues of the day" (ibid, p. 2). Agenda setting approaches to media influence therefore assert that media accounts "tell audiences not 'what to think' but 'what to think about'" (Vultee, 2011, p.80). This is important when viewed alongside the concept of the 'availability heuristic,' which suggests that audiences "assess the probability of an event by the ease with which occurrences can be brought to mind by recall or imagination," therefore "[f]amiliar, recent, or salient events seem more probable because they are more available to the mind than the less famous, older, or less dramatic events" (Chandler 2008, p. 127). This idea suggests that people react to the possibility of an event, rather than the probability, especially with respect to strongly negative events (ibid, p. 128). Therefore the choice of media frames and the space given to covering an issue may have an effect on audience perception of that issue.

This apparent influence on public opinion is important because the influence of mass audiences is a key component of exceptionalism. This is the state which securitization seeks to bring about, wherein 'exceptional measures' are used to manage a threat. Timothy Garton Ash makes this link more explicit, asserting that this state of exception is brought about by "an atmosphere of menace which the media help to transport and magnify" (in Huysmans, 2004, p. 324). Such exceptionalism "distorts the relation between the people and the leadership by more radically asserting the need for unity in times of crisis" (ibid, p. 333). 'Unity' results in the silencing of dissenting voices and thus the limiting of the possibility for democratic debate, and it can "collapse the gap between the people and political leaders [so that] [f]allibility and institutionalized slowness of decision-making give way to a sovereign leadership that necessarily speaks the infallible truth of and for the people" (ibid, p. 333-334). This results in "unrestrained and irrational mass politics [as]... the will of the people slips from a rationally and formally constrained contest of opinions to a violent and emotional assertion of a unity of opinion among the masses" (ibid, p. 335).

However as Dunn Cavelty notes, the idea of 'exceptional measures' is poorly defined by the Copenhagen School, which asserts that securitization can be taken to an extreme level through what Buzan et al. have termed 'hypersecuritization' (1998). This involves the "expansion of securitization beyond a 'normal' level of threats and dangers by defining 'a tendency both to exaggerate threats and to resort to excessive countermeasures'" (Hansen and Nissenbaum, 2009, p. 1163-1164). Ole Waever, one of the founders of the theory, identified a central conceptual weakness in this ‘extraordinary measures’ component, in that such measures are “highly contextual and subjective: they might not always be ‘security measures’ in a restricted sense, and security measures might not always be exceptional to everyone” (in Dunn Cavelty, 2008, p. 26). Hansen and Nissenbaum have also questioned the idea of exaggeration in this definition, suggesting that it implies that there are ‘real’ threats that are not exaggerated, and also pointing out that securitizations which are unsuccessful are often seen as exaggerated, whereas accepted securitizations are seen as ‘real’ (2009).

A more concrete understanding of ‘exaggerated threats’ can be found in Giorgio Agamben’s detailed historical analysis of the increasing use of ‘exceptions’ or the suspension of law as a response to insecurity, resulting in the expansion of the power of the executive and the erosion of freedoms (2005). He documents a shift in the way nations are governed, involving the gradual emancipation of a ‘state of exception’ from periods of warfare, through the declaration of a 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, p. 14). Examples of such suspensions of law can be seen in today’s War on Terror, wherein freedoms are restricted and minority groups targeted due to ‘necessity’, and these exceptions continue almost indefinitely due to the constant generalized anxiety produced by a never-ending war against a non-specific enemy. Agamben explains how,

> President Bush’s decision to refer to himself constantly as the “Commander in Chief of the Army” after September 11, 2001, must be considered in the context of this presidential claim to sovereign powers in emergency situations. If, as we have seen, the assumption of this title entails a direct reference to the state of exception, then Bush is attempting to produce a situation in which the emergency becomes the rule, and the very distinction between peace and war (and between foreign and civil war) becomes impossible. (ibid)

Another useful concept is that of ‘threat inflation’, a term taken from political science which refers to “the attempt by elites to create concern for a threat that goes beyond the scope and urgency that a disinterested analysis would justify” (Brito and

Watkins, 2011, p. 2). In Jerry Brito and Tate Watkins' examination of the role of the media in the run-up to the Iraq War, they claim that a securitizing framework promoted threat inflation rather than reliance on empirical research, as "[l]acking any clear *casus belli*, the administration sought popular and congressional support for war by promoting several rationales that ultimately proved baseless" (ibid). They warn that, "[w]hen a threat is inflated, the marketplace of ideas on which a democracy relies to make sound judgements—in particular, the media and popular debate—can become overwhelmed by fallacious information. The result can be unwarranted public support for misguided policies" (ibid, p. 2). They suggest that the media is particularly guilty of aiding threat inflation due to its tendency to conflate threats by referring to qualitatively different threats as if they are the same, and due to its repetition of unverified 'evidence'. This is a result of media conventions which tend to support the technification of a subject due to a reliance on 'expert' testimony.

This is not to say that the media has a 'hypodermic needle' effect wherein media frames inject messages into the minds of the audience. The propaganda models and ideas of 'mass persuasion' developed by Walter Lippman and Edward Bernays in the post-World War One period have long been abandoned in favour of more nuanced models of media influence which take into account the role of social, cultural, political and economic factors, as well as the role of public opinion leaders and individual differences in public opinion formation (Schiller, 1996). As Entman notes, "[c]ertainly people can recall their own facts, forge linkages not made explicitly [by the media], or retrieve from memory a causal explanation or cure that is completely absent from the text" (1993, p. 56). However he also notes research from Zaller (1992), Kahneman and Tversky (1984), and Iyengar (1991) which suggests that "on most matters of social or political interest, people are not generally so well-informed and cognitively active, and that framing therefore heavily influences their responses to communications" (1993, p.56). These findings suggest that the framing of an issue is likely to be accepted when the issue is not well understood by the audience. In the case of highly technical issues such as that of cybersecurity, a full understanding by the audience is unlikely, and therefore the mass dissemination of the securitizing framework by the media may encourage the acceptance of this frame as 'reality,' thus legitimizing emergency responses.

Fred Vultee has contributed important empirical research to the media effects field, specifically dealing with securitization (2011). His work expands on the body of research into the 'limited effects' of media, which examines the influence of factors internal both to the news article and to the individual reader on an audience's acceptance. By editing news reports so that they contained securitized or non-securitized statements about an issue, Vultee examined the likelihood of a securitization being successful according to the impact of frame and personal variables such as geographical proximity to the threat, scale of violence, association of the threat with 'terrorists', level of trust in the government, attention paid to security issues, and degree to which audience members considered their political stance to be aligned with that of the media (2011). His research indicated a high level of contextual influence, resulting in a situation where "[t]o speak security on an issue will not invoke security for all, but it appears quite able to invoke a particular security for some" (ibid, p. 92). This suggests that the success of a securitization is dependent not only on the speech act itself, but on a host of facilitating conditions external to its linguistic structure.

Therefore while it is clear that the media are well-suited to securitization because they have the ability to influence the opinion of an audience, external factors can mitigate this influence. Vultee's focus on the response of a mass audience to a securitizing framework is certainly important; however it assumes the acquiescent role of the media in the securitization process. A gap in the literature remains with regard to how different media organizations respond to such frameworks, and what degree of autonomy media institutions have in choosing to employ a securitizing frame to a news report. Institutional conventions of media may predispose it to securitization, however members of the media constitute an audience themselves who will also be subject to contextual influences that may have nothing to with the securitization, but may greatly affect its impact. Therefore an exploration of the external or contextual and social elements of a securitization can be used to assess the media's ability to question a securitizing move, and can also develop the contextual requirements of media effects research.

External, or Contextual and Social Elements: An Effect **in** *media*

The second facilitating condition has two main elements, the first of which has to do with the threat itself. As Buzan et al. note, “[i]t is more likely that one can conjure a security threat if certain objects can be referred to that are generally held to be threatening—be they tanks, hostile sentiments, or polluted waters. In themselves, these objects never make for necessary securitization, but they are definitely facilitating conditions” (1998, p. 33). This complements the media’s approach to news coverage, which involves a necessary reduction in the complexity of an issue, given the constraints of print space and airtime, through the referencing of existing schemas. Therefore it is common for news articles to use past events, terms, or phrasing to give the reader context and to quickly explain how an incident should be viewed, for example characterizing something as ‘terrorism’, or invoking Pearl Harbour, 9/11, or weapons of mass destruction. Unfortunately, this oversimplification can often result in threat conflation, or the repetition of unverified ‘evidence’ as Brito and Watkins have noted (2011). This is especially likely to be the case in media reports of ‘cybersecurity’ incidents, which are highly technical and thus difficult to explain to a lay audience in a short amount of time. In addition, Entman suggests that once specific terminology has gained salience, the use of a new term might result in a lack of understanding or an issue being taken less seriously, so there is an increased likelihood of threat conflation or the use of inaccurate terminology in cybersecurity (1993).

The second element of the external condition involves the position or social capital of the securitizing actor who usually speaks from a position of authority, for example political leaders, bureaucracies, governments, lobbyists and pressure groups. Although this does not have to be a position of official authority, as Buzan et al. have emphasized, the institutionalization of security has resulted in the accepted security expertise of members of the military, intelligence community, and government (1998). Norman Fairclough notes that speech act-based theories tend to understate “the extent to which people are caught up in, constrained by, and indeed derive their individual identities from social conventions” (1989, p. 9). He contends that, while actors do use conventions, they also follow them. Therefore explorations of securitization must emphasize “both the determining effect of conventions and the strategic creativity of individual speakers, without reducing the practice to one or the other" (ibid, p.9-10). This is especially important when considering the role of the media, which may not promote a securitizing actor's ideas with deliberate intent, but which is operating within conventions that limit its ability to question 'official' ideas.

The role that the media plays in supporting the authority of the securitizing actor has been explored by Piers Robinson, who states that "[a] wealth of critical literature written over the last 25 years maintains that the political and economic positioning of major news media institutions leads to a situation in which news accounts tend to support dominant perspectives" (2001, p. 525). Pan and Kosicki's highlighting of professional conventions of news writing sustain these assertions, as they suggest that "claiming empirical validity or facticity by quoting experts or citing empirical data" and "linking certain points of view to authority by quoting official sources" are common tropes of the media (1993, p. 60). The reliance of the media on official sources to legitimize news reports contributes to what Robinson refers to as "the ability of government to influence the output of journalists and the tendency of journalists to both self-censor and perceive events through the cultural and political prisms of their respective political and social elites" (2001, p. 525). This supports the 'manufacturing consent' school of thought which holds that "the media functions primarily to mobilize support for the policy preferences of dominant elites" (Robinson, 2001, p. 524; see also Chomsky and Herman, 1988; Hammond and Herman, 2000; Herman, 1993).

Similar conclusions are reached by John Kingdon in his study of effects on policy agenda; he notes that the media has a less-than-anticipated effect on the policy agenda due to the high turnover of stories in press coverage, thus diluting its impact. One of the journalists he interviewed explained: "[t]he press has the world's shortest attention span. We don't stick to a story for long enough to educate anybody. We move from one crisis to the next" (1995, p.59). In fact, the policymakers that Kingdon interviewed were of the opinion that the media became aware of policy developments only after they were already well underway, and that the media therefore could only report on what was already happening rather than shape the form that these policies would take. Kingdon explains that

> [t]he media's tendency to give prominence to the most newsworthy or dramatic story actually diminishes their impact on governmental policy agendas because such stories tend to come toward the end of a policy-

> making process, rather than at the beginning... the agenda was set much earlier and by processes not much affected by the media. (ibid, p.59)

Other interviewees stated that “media coverage is not critical” because policymakers in government “have alternatives of leverage on the system, and we don't have to use the media very much” but “the media will follow us because what we do makes news” (ibid, p.61).

Elite Dissensus

This assessment presents the weaknesses in the media’s ability to be critical of the views of securitizing actors. The similarities between media conventions and the facilitating conditions of securitization make clear that the media can assist in the promotion of a securitizing attempt, and is perhaps even predisposed to do so. However this does not entirely circumvent the media’s ability to act independently, or to make choices about the issues and views covered. Piers Robinson (2001) suggests that there is opportunity for the media—or other actors—to take a much more active role in the framing and dissemination of policy debate when dominant elites are not in agreement over the best approach to combating a threat. He terms this situation “elite dissensus.” This acknowledgement of the complexity of policy debate *prior* to a securitization attempt is missing from securitization theory, as Dunn Cavelty notes in her critique; the process through which an actor comes to speak security is underexplored (2008).

There are many U.S. institutions that have been created to manage different aspects of security, from the military, to state police, the Federal Bureau of Investigation, and the foreign and domestic intelligence agencies of the Central Intelligence Agency and the National Security Agency. Within these organizations are various departments and individual actors with different responsibilities and ways of viewing security threats. The so-called Paris School—scholars from the Institut d’Etudes Politiques de Paris—have noted that the Copenhagen School does not explain how it is decided which actor, of all the possible actors, will be the one to perform the securitizing speech act over a particular issue (in Dunn Cavelty, 2008). The Paris School therefore suggests that a broader group of potential securitizing actors must be identified, known as ‘professionals of security’ whose “voices are inherently endowed with more weight than others due to the symbolic capital at their disposal, which corresponds to their positions of authority" (ibid, p. 27). This understanding indicates that securitization is not simply a case of the mobilization of rhetoric, but also of resources. Such an understanding can account for the current turf wars that occur between different military, intelligence, and law enforcement branches as they attempt to legitimize their post-Cold War existence by creating new practices and institutions to deal with new threats such as cybersecurity (ibid). Dunn Cavelty explains that "this multiplicity of positions leads to struggles between competing discourses, the goal being to gain legitimacy and to become the dominant discourse" (ibid). The mobilization of resources to support this discourse can significantly affect who wins the discursive struggle and becomes the securitizing actor, thus legitimizing their continued existence. Kingdon's research supports this; he suggests that "[s]ometimes active participants in a bureaucratic process want to enlarge a conflict beyond the confines of usual channels. If they appear to be losing a battle, one way to turn the tide is to leak information to the press that would be embarrassing to their opponents" (1995, p.61). Therefore within this struggle, decisions made by the media over whose views to promote could make all the difference in who becomes the securitizing actor, and whose approach to the threat is legitimized.

This view of the role of media in securitization suggests that the media does not only reflect debate and dissensus over policy, but can in fact become an active player in the creation of policy. Piers Robinson points to broader policy studies literature which suggests that there is a correlation between policy dissensus and "the ability of 'external' actors to influence policy formulation" (2001, p. 533), while research from George (1980) and Hilsman (1987) suggests that policy-making is "the outcome of a complex bargaining process between a set of subsystems in government" (ibid, p. 535). Communications research has demonstrated that the media can be used as a tool during times of policy uncertainty; Tuchman notes that officials will sometimes call themselves 'reliable sources' and "anonymously float an idea in the mass media in order to gauge the reactions of other cabinet officers, senators, or citizens to a potentially controversial program" (1978, p. 4). This is corroborated by Kingdon's research, which suggests that policymakers often communicate indirectly, and that "one way to bring an idea to the attention of someone else... is to be covered in the pages of the major papers" (1995, p. 59).

However Robinson suggests that the media could play an even more active role in policy creation; an idea he has explored in his *policy-media interaction model*. He suggests that elite dissensus over an approach to an issue can result in negative media coverage of the government, which brings the possibility of public opinion being influenced by the negative press. This can in turn result in damage to the government's image and credibility, and policy-makers might start to question the cogency of existing policy (Robinson, 2001, p. 535). If dissensus is a result of disagreement over policy, then the media can provide additional bargaining power to either side of the debate. If adequate policy simply doesn't exist, pressure from media coverage can push policy-makers to create policy without full consideration of its implications, rather than be 'caught on the hop' (ibid). And finally, without an established official line, government is ill-equipped to respond to journalists, causing policy-makers to be even more vulnerable to a hostile press (ibid), therefore the swift resolution of elite dissensus is even more important. This is supported by Kingdon's findings that “media attention to an issue affects legislators' attention, partly because members follow mass media like other people, and partly because media affect their constituents” (1995, p.58). Unfortunately this model suggests that the media’s ability to exert influence on policy may be limited to incidents of policy dissensus, and extends only to choosing to support one of the various official viewpoints in a policy debate. This is reflective of Entman's contention that “[d]issenting opinions are not necessarily shut out, but they have a better chance of being aired if they reflect a dissent that has already begun among elites (in Vultee, 2011, p. 82). In fact Robinson notes that “if government policy is decided on, policy-makers are likely to resist the pressures of negative media coverage. Indeed, policy-makers are more likely to work harder to sell existing policy by drawing upon their substantial resources and credibility as an information source in order to influence media debate” (2001, p.535).

This emphasis on the 'selling' of policy highlights the importance of framing which is largely missing from Kingdon's account of media influence on policy agenda setting. Dunn Cavelty posits that not all problems are propelled onto the security agenda, meaning that the media may be able to influence not only how the threat is characterized, but also which threats are securitized at all. In addressing the question of why an issue is taken up, discursively fought over, and finally securitized by an actor, she uses Kingdon’s agenda-setting theory to illustrate the conditions which allow for an issue to be moved onto the security agenda when there is a ‘policy window’ (2008, p. 33-34). Such a window, or opportunity for attention to be given to a specific issue, opens either due to a change in the political stream, or when a new problem comes to the attention of officials (ibid, p. 34). In the latter case, societal conditions that are less than ideal must come to be perceived as serious problems; this can occur in one of three ways. The first possibility is through an *indicator* “in the form of statistics, particular studies, or budgetary impacts that shows clearly that there is a problem” (ibid, p. 34). Secondly, *focusing events* can occur in the form of a disaster or crisis. And finally a shift in perception can be caused by *formal and informal feedback*, which refers to “systematic monitoring and evaluation studies... or complaints or routine casework” (ibid). These are just the sort of events that are covered in the media, and so choices made by media agencies as to whether and how to report on these occurrences can affect how an issue is viewed when it is placed on the policy agenda (Robinson, 2001).

This analysis suggests that while the media may not be able perform a securitizing move by itself, its position as mediator between the securitizing actor and an audience who must accept the securitization indicates a potentially significant role in this process. The Copenhagen School would define this role as that of a ‘functional actor’. This role is extremely important because it allows the media to have an effect on the likelihood of a securitization’s success by their accepting or questioning this framing, and either repeating it or framing the apparent threat in an alternative way. It has been noted that the media has a level of autonomy in the way it chooses to frame events. While media convention may predispose it to supporting official perspectives, multiple other factors affecting individual news sources will also play a role, and within the frame of a debate, the media can choose to support one perspective over another.

This is important because of the potentially damaging effects of a successful securitization. As has been made clear, security involves a degree of sacrifice. Framing Internet-based risks as posing a threat to national security legitimizes responses that increase control and surveillance as a way of minimizing risk. However such responses threaten to reduce privacy and freedom of speech, as the availability of surveillance systems could result in the legitimization of ever-widening surveillance dragnets, especially in the context of terrorism, where everyone is potentially suspect (Lyon, 2003). At the same time, once established the original purpose could be distorted and expanded in a process Langdon Winner refers to as 'function creep' (1977), leading to the application of surveillance systems to progressively less extreme circumstances like copyright infringement (Parsons, 2012). The media’s choice to highlight the costs to privacy and civil liberties or to encourage their acceptance as necessary, or even to ignore these costs altogether, could change the way the public views and discusses these responses. The process through which an issue is framed as relevant to national security must therefore be examined, and the concept of security denatured, if we hope to have a frank discussion about the costs and benefits of security actions. The media may be one space in which this discussion can occur.

Chapter 3.

Facilitating Conditions: Historical Context

> Within a quarter of an hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed...Freight trains have derailed... Aircraft are literally falling out of the sky... The financial system has also frozen solid... And the U.S. military is a series of isolated units, struggling to communicate with each other. Several thousand Americans have already died, multiples of that number are injured... (Clarke and Knake, 2010, p.67)

This chaotic scene is the potential aftermath of a major cyberattack on the U.S., according to Richard A. Clarke, who served as the National Coordinator for Security, Infrastructure, and Counter-Terrorism under President Clinton and again as the Special Advisor to the President for Cybersecurity under President George Bush Jr. According to this 'cyber-doom' logic, any infrastructure that relies upon a digital system is vulnerable to a cyberattack. The belief in cyber-disaster scenarios caused President Obama, during his 2008 presidential campaign, to declare the U.S. information infrastructure a ‘strategic asset,’ a move which positioned the Internet as a significant issue for the military (Clarke and Knake, 2010, p.116). This is problematic because, as James Lewis of the Center for Strategic and International Studies (CSIS) points out, “it is not at all clear that a military response [to cybersecurity challenges] is either appropriate or effective” and that most of what is included under the term ‘cyberwar’ “are really acts of crime, espionage, or political protest” (in Lawson, 2011, p.22). The depiction of such scenarios, it has been argued, is a reaction to a perceived lack of attention by policymakers to computer-mediated threats, resulting in emotional appeals in order to prompt a reaction (Lawson, 2011, p.1; Dunn Cavelty, 2007b). Much of the research on cybersecurity has been accepting of the idea that a cyberattack could cause widespread chaos, though authors differ in their assessment of when future attacks may occur, or if they are even possible

(Dunn Cavelty, 2007b). Therefore this chapter will address the factors—or to use the language of the Copenhagen School, the external 'facilitating conditions'—that promote the acceptance of securitizing and even hypersecuritizing discourse in discussions of networked computer security in the media. By providing an account of the external context within which media reports of cybersecurity issues are framed—thereby highlighting the complexity of the social, institutional, and political-economic influences on a successful securitizing speech act—an overly deterministic media effects model can be avoided.

This chapter will outline the history of the relationship between networked computing and the military, and will argue that computer security has been increasingly brought under the purview of the defense sector, resulting in its resignification as 'cybersecurity'. As a result, military logic has shaped popular understandings of the strategic importance of these technologies, and media groups may have difficulty contradicting or questioning the national security framing of developments within the field of networked computing. Computing—especially networked computing—and the systems and organizations that created and support information and communication technologies (ICTs), have a long and rich history with the defence sector and with security issues. The first packet switching network, ARPANET, was the result of a military-funded project that aimed to solve a national security problem. However, when this network became a public resource, the military relinquished its oversight. The subsequent explosive growth of the Internet, its integration into society and its eventual designation as a ‘strategic asset’ integral to the functioning of critical infrastructure, have resulted in an attempt by the defense community to re-establish control over the Internet. Many scholars have argued that “prior conventional wisdoms about the open, liberal character of the Internet and its many attendant consequences reflect less some inherent “nature” than they do the properties of the technology at a specific moment in time” because “code is not neutral or transparent but actively shapes what can be communicated and how” (Deibert, 2003, p.3-4; see also Lessig, 2000). While this is true, the shift away from the idealized 'lawless frontier' of cyberspace towards a more controlled Internet should be seen less as a new development and more as a return to the origins of networked computing. The application of a national security discourse to networked computing is not simply an attempt to address a new security concern; rather, an understanding of communications history allows us to interpret the current situation as a 'resecuritization' of the Internet, prompted by new social, technical, and global developments.

These external influences on the media's representation of established frameworks will be examined in three parts; to begin, the chapter will address the development of the military-industrial complex and its relationship to what is now being referred to as the 'cyber-industrial complex' (Brito and Watkins, 2011). This relationship between security, money, power, and technological development is central to the development of the cybersecurity field. The next section will address conceptual shifts and historical developments within military and technology sectors which have resulted in the emergence of three dominant cybersecurity concerns as defined by Helen Nissenbaum (2005). The first concern is that the digital infrastructure itself is threatened and faces attacks that could result in complete debility. This will be contextualized through an examination of the centrality of communications to national security. The second concern is that critical societal infrastructures—including banking, transportation, the power grid, communications, healthcare, and government among others—could be targeted and made vulnerable by virtue of their connection to and dependence on the digital infrastructure. This will be examined by looking at changes to the way wars are fought, also known as the revolution in military affairs, or the informationalization of war. The third concern will is that networked computing provides opportunities for the encouragement, organization, and implementation of disruptive and dangerous activities including terrorism. This will be examined as an effect of the broadening scope of national security, resulting from the changing nature of security threats. In the final part of the chapter, John Kingdon's agenda setting theory will be used to highlight how these shifts allow for an opening of a 'policy window' through which specific cybersecurity issues can be moved onto the political agenda, and the ways in which the media is predisposed to assist in that move.

Cyber-Military-Industrial Complex

According to Jerry Brito and Tate Watkins, the government "is expected to spend $10.5 billion per year on information security by 2015, and analysts have estimated the worldwide market to be as much as $140 billion per year. The Department of Defense has also said it is seeking more than $3.2 billion in cybersecurity funding for 2012" (2011, p.24). While demonstrating the level of concern attributed to cyber-vulnerabilites, these numbers also suggest heavy financial investment in a growing cybersecurity industry. The government has long been dependent upon military contractors to provide the research and production of advanced military technology, and Brito and Watkins argue that cybersecurity is the latest threat upon which the burgeoning military-industrial complex has focused its attentions. The relationship between defence, research and development (R&D), and private industry is therefore important to examine, as these groups all have a vested interest in the development of the field of cybersecurity. By taking a historical look at the technology industry, we can see that war has been the rallying call for industrialization and mass mobilization of the labour market towards a specific goal. The First World War prompted the mobilization of mass industrial power and facilitated the longterm implementation of Taylorism in American factories (Whyte, 2010). Chris Hables Gray notes that while Taylorism met with worker resistance, "worker's strikes and anti-Taylor legislation from pro-labor members of Congress were swept away by the U.S. entry into World War I. Militarization consolidated Taylorism in the arsenals and in many other industries" (1997, p. 118). Merritt Roe Smith tells a similar story in examining the implementation of Fordist management practices. He claims that "[t]he history of virtually every important metalworking industry in nineteenth-century America – machine tools, sewing machines, watches, typewriters, agricultural implements, bicycles, locomotives – reveals the pervasive influence of military management techniques" (in Gray 1997, p. 118).

This ramping up of industry as facilitated by warfare was paralleled by developments in the way universities functioned. In his history of the information age, Wade Rowland notes the shift in universities towards a targeted research and development model throughout the twentieth century (2006, p.100). David Noble explains that the aims of corporate engineers were not only to "standardize specific industrial processes and secure corporate command over the patent system" but also to "direct the human processes of scientific research and to create an educational apparatus which could meet the demand for research manpower" (1977, p.168). He also cites corporate engineers as "[leading] industry and schools in effecting close industry-university cooperation over matters of curriculum and recruitment" (p.168-169). This link between university research and industry development was clearly articulated during the First World War, which provided a "unique opportunity" due to its ability to unite under a common goal individuals and corporations who had previously been in competition, resulting in "an entire community as a single working plant for the purpose of organizing it for the most intelligent production of human wealth" (Charles Mann in Noble, 1977, p.207).While this perspective is somewhat idealistic, and ignores the competition that could and obviously did result from military contracts, it illustrates the attitude which resulted in the incorporation of higher education into the military-industrial complex. By late 1916 the Naval Consulting Board, the Council of National Defense, and the National Research Council had devised a personnel index of available manpower, and the following year the Intercollegiate Intelligence Bureau was formed to "facilitate the ready placement of college men (particularly graduates) in the government service" (ibid, p.207).

The Cold War was a boon for the military-industrial complex, providing a constant threat in the form of the Soviet Union and the possibility of nuclear war, which legitimized the massive build-up of weaponry to deter the apparently imminent attack. The increasing outsourcing of military research and development to corporations or, as Peter Singer puts it, the 'privatization of the military,' is now a common solution to the limitations of military resources. However it is problematic because of the motivations of private industry as opposed to the publicly-run military. Singer explains the distinction thus:

> Traditionally, the government provides all its citizens with certain services, which are generally paid for through taxation. This takes place in what is known as the public sector. In contrast, in the private sector, individual citizens, now known as consumers, purchase needed goods and services in an open market, paying with their own discretionary funds. This market is made up of private firms motivated by profit. Thus, the distinctions between these two sectors are the sources of funding, the nature of the relationship between provider and user, and the employment status of the deliverers. (Singer, 2003, p.7)

The power of this union of military with capital was acknowledged by President Eisenhower in his 1961 farewell address, in which he warned against the "acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex" and that "in holding scientific research and discovery in respect, as we should, we must also be alert to the equal and opposite danger that public policy could itself become the captive of a scientific-technological elite" (in Der Derian, 2001, p.viii). Frank Fischer (1990) notes the dangers of living in such a 'technocracy', wherein "technically trained experts rule by virtue of their specialized knowledge and position in dominant political and economic institutions" (p.17) and "governance becomes less a matter of determining the appropriate direction for society than one of adjusting its institutions and policies to the flows of economic and technological development" (p.16). According to Brito and Watkins, a 'cyber-industrial complex' may be emerging today. They note that "[i]n 2009 the top 10 information technology federal contractors included Lockheed Martin, Boeing, Northrop Gruman, General Dynamics, Raytheon, SAIC, L-3 Communications, and Booz Allen Hamilton" (Brito and Watkins, 2011, p.25), highlighting the consistency between traditional military contractors and those relied upon for information technology today. They note how the military-industrial complex was able to grow because it facilitated mutually beneficial development, as "[m]ilitary expansion and increased defense spending help grow Pentagon budgets and provide steady revenues to defense contractors. They also allow congressmen to win constituents' approval by sending appropriations and jobs back home" (ibid, p.21). This relationship can be seen today in the competition over the location of the permanent headquarters of the new U.S. Cyber Command. Brito and Watkins note that, despite cuts to traditional defense spending, cybersecurity has opened up a new industry for spending. Investment in this field would have a knock-on effect on the economy of the state that hosts this industry. As a result "[i]t was estimated that Cyber Command headquarters would bring at least 10,000 direct and ancillary jobs, billions of dollars in contracts, and millions in local spending" (Brito and Watkins, 2011, p.27).

As technologies and the society that depends on them become more complex, the reliance on technical experts and the industries that support them grows. Dallas Smythe has noted the integration of transnational corporations (TNCs) with the Department of Defense and national government structure and policy as demonstrated by the mobility of executives, lawyers, engineers, and scientists between these sectors (1986, p.70). An example of this mobility today can be seen in the career of Mike

McConnell, a former vice admiral in the U.S. Navy who also held the position of Director of the National Security Agency from 1992-1996, and served as the Director of National Intelligence between 2007 and 2009, while before and after his appointment as DNI, he had been the Senior Vice President of military contractor Booz Allen Hamilton (Wright, 2008). So long as profit is the motivating force behind the provision of military resources, there will be a tendency to promote conflict rather than to solve it, so as to ensure a steady stream of revenue. This is similarly the case for the military itself: conflict is needed to justify its existence and to legitimize its influence. Therefore claims that the national security of the United States is threatened due to the vulnerabilities of cyberspace must be viewed critically, because while valid concerns do exist, they may be manipulated due to the imperative to guarantee continued cybersecurity development and profit.

Communications in Warfare

The first category of cybersecurity concern that Nissenbaum (2005) highlights is that U.S. digital infrastructure itself could become a target in warfare, and faces attacks that could result in complete debility. This concern with the vulnerability of a national digital communications system is a logical one given the fact that communications systems and the information they provide have long been a central part of warfare. The endless quest to eliminate the inherent uncertainty in military operations, often referred to as the 'fog of war', is evident throughout military history, as each side strives for the tactical advantage of informational awareness (Van Creveld, in Arquilla and Ronfeldt, 1993, p. 58). RAND Corporation analysts John Arquilla and David Ronfeldt draw from past examples of the centrality of communications to warfare in order to develop a theory of the way in which new information and communication technologies are enhancing an age-old strategy of information dominance. They argue that during the Second Punic War of the 3rd Century B.C., “[b]etter communications contributed significantly to the ability of Hannibal’s forces to win a string of victories over a period of sixteen years” and that “[i]n the most dramatic example of the use of superior information, Hannibal’s relatively small forces were able to rise literally from the fog of war at Lake Trasimene to destroy a Roman army more than twice its size” (ibid, p. 33). Similarly, the targeting of an enemy's communications technologies has been instrumental to maintaining information and by extension tactical dominance, as demonstrated in the Napoleonic Wars by the British army's raiding of French semaphore signalling stations, and then striking while French communications were disrupted (ibid, p. 33).

The attempt to use new communications technologies as a tool of national security dates back to at least the beginning of the Cold War, when the National Security Agency was created with the sole task of encoding and decoding communications intelligence (Saco, 1999). Similarly, Myriam Dunn Cavelty has highlighted the growing awareness in the United States of the importance of reliable telecommunications to national security, which she traces back to the Cuban Missile Crisis in 1962, “when difficulties in terms of communication between the United States, the Soviet Union, NATO, and other national leaders threatened to complicate the crisis even more” (Fursenko and Naftali in Dunn Cavelty, 2008, p.41). Shortly thereafter, an investigation of communications systems which “served national security needs” resulted in President Kennedy issuing a Presidential Memorandum establishing the 'National Communications System' (Dunn Cavelty, 2008, p. 41). Its mandate involved “linking, improving, and extending the communications facilities and components of various federal agencies in order to further the interconnectivity and survivability of vital information infrastructures” (ibid, p. 41-42). This rationale, emphasizing the need for communications in emergency management and response, mirrors the imperative for the creation of the system of networked computers which were a precursor for the modern-day Internet.

While the Internet has its origins in the military ARPANET, the communication network it developed into was not a military creation. Nor was it the intention of the public bodies who were given control of the ARPANET project that the network would be used as a medium for interpersonal communication. In fact it was designed “to allow scientists to overcome the difficulties of running programs on remote computers” (Abbate, 1999, p. 2), but it evolved into something far more communication-oriented through what Janet Abbate terms “an unusual and sometimes uneasy alliance between military and civilian interests” (ibid). In her history of the Internet, Abbate tells the story of the transformation of the Internet from a relatively small set of networks with connections to defence research or operations, into a mass of civilian controlled, privatized networks which became our modern day Internet. The Internet was not the first military-funded technology to become popularized and appropriated by civilians; rather as Dallas Smythe argues, there is a long history of military-funded research and development which has resulted in the creation of some of the major technologies upon which our society relies today. Military projects are reappropriated or "profitably spun-off" and tailored to a civilian market (1986, p.69). For this reason, Smythe proposes that the capitalist war-machine be termed the 'military-civilian-industrial complex' (MCIC), due to the central role of civilians in the creation of technologies by the military-industrial complex. He argues that "the prime mover (institutionally speaking) is the creation and management of a nonmarket demand for military goods which is linked to the creation and management of market demand for goods in the civilian markets" (ibid, p.66). To illustrate, Smythe gives the example of aeroplanes; the research and development of bomber planes for warfare was subsidized by the military, and from this research passenger aeroplane designs were created (ibid, p.69).

Smythe notes that the shift of military projects into civilian markets is a trend that is particularly prevalent in the field of communications; much of the technological development during World War 1 was reliant on the federal funding for research and development. For example Smythe argues that the eventual creation of the transistor, which was central to the development of radio communications, would not have been possible without the funding Bell Telephone Laboratories received as one of the largest military contractors (ibid, 69). Similarly, computing was developed due to the need for rapid fire-control of anti-aircraft artillery, again demonstrating the "endless flow of research and development money from the military budget to the [transnational corporations], which promptly established business empires providing hardware and software for communications both for military and, as a lower priority, for civilian use" (ibid, 70). Though creation of the Internet began as the U.S. military research project 'ARPANET', it quickly expanded under the influence of the international computer research community and developed into a bigger, more flexible and decentralized system (Abbate, 1999, p. 113). The work of Vint Cerf, Robert Kahn, and others on internetworking—the ability to transmit packets of data between different technically incompatible networks—resulted in the creation of TCP/IP, the standard host protocol upon which the Internet is built. However, "few people outside the computer science community had even heard of the ARPANET in the early 1970s, and fewer still could have recognized that the Internet would someday become an important public and commercial technology" (ibid, p. 127). In the following years, many separate networks and bulletin board systems (BBS) were independently developed, indicating the wider commercial potential of networked computing not only for communication and research, but also for making new friends, sharing ideas, and finding communities (Sterling, 1992). However, even at this early stage, there was concern that sensitive information might be stolen by malicious actors, prompting the separation of the military users of ARPANET—who desired strict access controls—from the academic researchers of the network who favoured open access" (Abbate, 1999, p. 142). Once sensitive military activities were separated into their own network, the potential was much greater for ARPANET to be transferred to civilian control, and the need for similar levels of security on a civilian network was not given consideration. This shift distanced networked computing from the idea of security, as ARPANET became a public utility and no longer a military and, by extension, a security medium.

When the military relinquished control of ARPANET, it was a research tool used mainly by academics according to strict guidelines, and commercial use was not permitted. There was no anticipation of the way it would change and grow, becoming central to the functioning of society and thus becoming a source of vulnerability for the nation. Computers at that time were very basic- the first personal computer, the Altair 8800, was made available in 1975 as a DIY project for hobbyists; it often didn't work, had no screen, and was programmed by flicking little switches on and off. By 1977 there were some ready-made computers on the market, such as the Apple II, but it wasn't until 1981 that IBM entered the market and made its PC the industry standard (Abbate, 1999, p. 186). When single-user computers became available and technological advances led to the creation of graphic interfaces, keyboards, and the mouse, demand for computers surged and with it, a desire for local area networks to connect to them (ibid, p. 187). However, this was still a long way from the level of network dependence we have in our current society, so it is unsurprising that the first conversations about network security occurred in technical circles, and were concerned with the integrity of the network, rather than the implications of security threats for wider society.

Considering the rapid growth of the computer industry and the increasing automation of many areas of society since the 1980s, there is an element of inevitability in the renewed military interest in the Internet and the security risks associated with networked computing. Ralf Bendrath explains how the terminology around computer security shifted in the 1990s, drawing strong connections between the threats posed to network security and historical threats to the state (2003, p. 50). Cybersecurity expert Winn Schwartau claims to have coined the phrase ‘electronic Pearl Harbour’ in his 1990 testimony to Congressional Subcommittee on Technology and Competitiveness, Committee on Science, Space and Technology (Schwartau, 2012). He similarly claims to have aided in the mainstream adoption of the term ‘information warfare,’ which was previously a military term (ibid). Also in 1990 the National Academy of Sciences produced a report on computer security which employed a strong securitizing discourse. It began, “[w]e are at risk. Increasingly, America depends on computers... Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb” (Bendrath, 2003, p. 50; see also Hansen and Nissenbaum, 2009). A few years later these concerns were more clearly articulated in the 1996 Joint Chiefs of Staff publication, “Information Warfare: A Strategy for Peace... the Decisive Edge in War”, which explained how “the seamless relationship [between the US National Information Infrastructure and the Defence Information Infrastructure] makes distinguishing between them impossible. They share terrestrial telecommunications networks, a variety of information databases, and satellite communication networks. These infrastructures connect geographically separated forces and span international boundaries” (p. 2). The Joint Chiefs' contention that “[u]se breeds dependence, dependence creates vulnerability” (ibid, p. 1) neatly sums up the shift in emphasis from networked communications as a strategic asset, to a point of national vulnerability.

Changing Nature of War, or The Revolution in Military Affairs

The second concern that Nissenbaum highlights is that critical societal infrastructures could be targeted and made vulnerable by virtue of their connection to and dependence on digital infrastructure. This new fear highlights the aforementioned shift in the way the Internet is thought about; the military's attitude towards ICTs on the battlefield moved from their conceptualization as a 'force enabler' or a 'force multiplier', to being seen as a source of vulnerability (Dunn Cavelty, 2008, p. 41). Initially, the dominant idea was that ICTs could provide the essential information advantage in warfare. Bruce Berkowitz suggests that “the Information Revolution has fundamentally changed the nature of combat. To win wars today, you must first win the information war” (2003, p. xi). As we have established, information dominance and superior communications have always been central to warfare and to national security, however the advance of technology coupled with the creation of weapons of mass destruction in the second half of the 20th century reenforced this imperative. The use of nuclear weapons on Hiroshima and Nagasaki during the Second World War both realized and ended the idea of ‘total war'; mutually assured destruction or ‘MAD’ ensured that total war was no longer viable in nuclear-armed states (Gray, 1997, p. 168). During the Cold War, the logic of deterrence held that the leader in the arms race could be determined by comparing numbers of tanks and missiles between the U.S. and the Soviets; however this idea was questioned by Andrew W. Marshall, who contended that “[c]ountries playing offense need different weapons from countries playing defense” (Berkowitz, 2003, p. 33). Albert Wohlstetter expanded upon this idea, suggesting that “even the strongest army or air force could have an Achilles' heel” and that “a critical flaw, astutely exploited by an opponent, could leave even the most powerful military force dangerously weak” (ibid). This concept of 'asymmetric threats', wherein a much stronger force could be defeated by a weaker opponent, became a popular alternative to the impossibility of total war and the endless race to mass ever more weaponry. The development of computing therefore became central to gaining information dominance so as to ensure that the blows struck are at the opponent’s weakest point. As Berkowitz puts it, “control the information flowing through your adversary's computers and communications networks, and you could control the outcome of a battle or a war” (2003, p. 30).

Modern computing was a solution to this desire for control and certainty in conflict, developing through the military-industrial partnership which grew in force during the Cold War. Paul Edwards contends that “computers created the technological possibility of Cold War and shaped its political atmosphere” while at the same time, the Cold War shaped computers: “[i]ts politics became embedded in the machines—even, at times, in their technical design—while the machines helped make possible its politics” (1996, p. ix). The ability for computing to provide the desired control and therefore security by dispersing the so-called 'fog of war' was firmly established during the Cold War, as Edwards argues in a summary that is worth quoting at length:

> As machines, computers controlled vast systems of military technology central to the globalist aims and apocalyptic terms of Cold War foreign policy. First air defenses, then strategic early warning and nuclear response, and later the sophisticated tactical systems of the electronic battlefield grew from the control and communications capacities of information machines. As metaphors, such systems constituted a dome of global technological oversight, a *closed world*, within which every event was interpreted as part of a titanic struggle between the superpowers. Inaugurated in the Truman Doctrine of “containment,” elaborated in Rand Corporation theories of nuclear strategy, tested under fire in the jungles of Vietnam, and resurrected in the impenetrable “peace shield” of Ronald Reagan’s Strategic Defense Initiative, the key theme of closed-world discourse was global surveillance and control through high-technology military power. (1996, p. 1)

The themes of control, total information awareness, and surveillance highlighted in this paragraph are perhaps even stronger imperatives today, as the asymmetric threat has moved from purely one of differently sized and armed militaries, to militia groups, terrorist groups, and suicide bombers who act outside the parameters of traditional warfare to avoid U.S. strengths, making the idea of a 'front' obsolete and blurring the lines between civilians and soldiers. Writing in the *Bulletin of the Atomic Scientists*, Eric Arnett tried to make sense of the implications of ICTs on this new warfighting landscape, suggesting that the superior processing power of computers would allow for ‘cyberwars’, which in turn would created a more fast-paced kind of warfare which he termed 'hyperwar'. He predicted that these technologies would allow for the progressive separation of man and machine, as ‘autonomous’ weapons such as smart bombs and planes without pilots were developed. Vast amounts of data would be collected from the field by sensors and processed by computers, meaning that humans would be increasingly reliant on the interpretation provided by these computers due to their inability to process such volumes of data themselves (Arnett, 1992 p. 15). His predictions were not far wrong. One of the earliest examples of this kind of use of computers was the Vietnam War, when the Ho Chi Minh trail was littered with sensors designed to detect all kinds of human activity from motion and body heat to the scent of urine, in an attempt to locate and destroy the ellusive North Vietnamese army. However despite the $1 billion a year that was poured into 'Operation Igloo White', and claims of the destruction of over 35,000 North Vietnamese trucks carrying supplies to the insurgency in South Vietnam, following “more than four years of intensive computer-controlled bombardment of their heavy-equipment supply lines, the communists were able to field a major tank and artillery offensive inside South Vietnam in 1972" (Edwards, 1993, p. 4).

A criticism of Arnett's definition of 'cyberwar' and its application in Vietnam is that it allows for a divorce of 'cyber' from 'war', so the emphasis is placed on the role of the technology. As Chris Hables Gray has noted, revolutions in military affairs "require a transformation of episteme as well as techne", or a "change the way we think about war, not just how we wage it" (2005, p.1). John Arquilla and David Ronfeldt agree with this idea and offer an important caveat for the assumption that technology is a force multiplier: technology enhances strategy, therefore it is not so much the hardware that is important as the enhanced strategy that it allows. Information technology in the battlefield allows for greater decentralization, as all personnel are networked through a variety of communication technologies. At the same time the increased flows of information can allow for greater 'topsight', meaning that strategy can be formed by central command with a fuller understanding of the situation, while tactics can be left up to more independent teams in the field, as different situations permit. Because of this, they see the Vietnam War as an example of the unsuccessful use of new technology. They argue that new technology gave the U.S. superior communications, which allowed for greater knowledge and topsight, but this encouraged a much more active role of the geographically distant central command, which used this enhanced knowledge to decide not only on strategy but also on tactics. Conversely the North Vietnamese military used communication for strategic central control (or topsight) but allowed those in the field to decide tactics with greater flexibility (decentralization) (1993, p. 39).

Edwards suggests that the mishandling of technology during the Vietnam War was due to the unique context of Cold War nuclear paranoia, in which "quantitatively oriented "scientific" administrative techniques, and the global objectives of U.S. military power combined to drive forward the centralization of command and control at the highest levels" which created "serious—and in the case of Vietnam, finally fatal—impediments both to effective action and to accurate understanding of what was going on in the field" (Edwards, 1996, p. 6). For Arquilla and Ronfeldt, the earliest and most successful example of the force multiplying potential of new technologies came in 1992, with 'Operation Desert Storm' during the Gulf War. This was the first conflict in which an army came close to operating a truly networked communications system, using local radio, military satellite, and commercial satellite. Enemy communications were largely destroyed, leaving the U.S. army to outflank the Iraqi forces because they knew exactly where the enemy was and the enemy had no idea where they were. Around the same time as Arnett was focusing on the new possibilities of technological warfare, Arquilla and Ronfeldt coined the term ‘cyberwar’ to describe networked war-fighting as a new phenomenon (Arquilla and Ronfeldt,1996).

While new ICTs were generally seen as force enablers in the early days of networked computing, there was still some concept of the potential vulnerability that networked computing could introduce to the nation. For example Tom Rona, a professor at MIT who worked on early networked computing, also saw the potential for these networks to become targets themselves. As Berkowitz explains, Rona understood that,

> any widget that collected, moved, or processed data was part of a system, each dependent on the other. He could also see that every widget in a system was a potential point of vulnerability, as was the information that passed through them. These so-called support systems were potentially a better target than the weapon itself. (2003, p. 29-30).

Berkowitz notes that this thinking was new, probably due to the unfamiliar concept of computers talking to each other, but it meant that if an army could control the information moving through an enemy's computer networks, it might be possible to control the outcome of a war (ibid). This idea expanded a strategy of war that had been used for centuries; targeting an enemy's communication system. The interception and codebreaking of German communications proved essential to the British war effort during World War One—a method that was facilitated by the cutting of undersea cables, leaving the Germans with few alternative communication options (Berkowitz, 2003). The targeting of communication systems was also central to the German Blitzkreig doctrine of World War II, wherein mass bombings were carried out as it was understood that “[d]estruction of this central (communications) nervous system is tantamount to destruction of the army” (Arquilla and Ronfeldt, 1996, p. 38). The difference with modern-day networked computing is that a physical attack on the communications infrastructure is not necessary; an attack could be carried out remotely, with little investment and little risk to those carrying out the attack. As Wesley K. Clark and Peter L. Levin put it, “[t]here is no form of military combat more irregular than an electronic attack: it is extremely cheap, is very fast, can be carried out anonymously, and can disrupt or deny critical services precisely at the moment of maximum peril" (2009, para. 3). This growing understanding of the vulnerability of the system necessitated a rethinking of where the battlelines were drawn; war could no longer be confined to the battlefield.

Changing Nature of National Security

While cybersecurity was developing as a major concern in the context of warfare, the expansion of the concept of national security allowed for the consideration of the defensive implications of computer security in a more general context, and provided justification for the argument that the security of the civilian Internet should come under the purview of the defense community. This is at the heart of the third concern that Nissenbaum highlights; that the Internet could be a resource for the organization and implementation of subversive acts (2005). The securitization of domestic issues can be seen throughout history; there are many examples of the executive taking control of civilian sectors for the good of the nation during times of unrest and therefore setting a precedent for future expansions of federal government jurisdiction. This began with the gradual separation of emergency powers from a 'state of exception' wherein the rule of law is suspended. According to Agamben’s account, use of the state of exception to facilitate the creeping expansion of executive powers began as far back as the U.S. Civil War, when President Lincoln “acted as an absolute dictator,” suspending the writ of habeas corpus along military lines between Philadelphia and Washington, imposing censorship of the mail, and authorizing the arrest and detention in military prisons of those suspected of being disloyal. After Congress ratified his actions, he proclaimed the emancipation of slaves, and generalized the state of exception throughout the territory of the United States (ibid, p. 20-21). According to Agamben, “the president openly justified his actions as the holder of a supreme power to violate the constitution in a situation of necessity” (ibid). During World War One, President Woodrow Wilson took even broader powers, not by ignoring Congress, but by having the powers in question delegated to him each time: “from 1917 to 1918, Congress approved a series of acts (from the Espionage Act of June 1917 to the Overman Act of May 1918) that granted the president complete control over the administration of the country” (ibid). Thus rather than declaring a state of exception as Lincoln had, he preferred to have exceptional laws issued (ibid, p. 21). This allowed him to use a generalized state of anxiety to pass specific laws, giving greater permanent powers to the executive without the President having to become a 'dictator.'

These actions broadened the scope of national security by separating emergency powers from a state of exception, but an even more significant shift came with the discursive attachment of these powers to periods of civil unrest, rather than war. Agamben explains that “[b]ecause the sovereign power of the president is essentially grounded in the emergency linked to a state of war, over the course of the twentieth century the metaphor of war becomes an integral part of the presidential political vocabulary whenever decisions considered to be of vital importance are being imposed” (ibid, p. 21). Therefore, the rhetoric of war, or the discourse of securitization, becomes connected to the ability to make potentially unconstitutional changes in law. During the Great Depression, President Franklin D. Roosevelt took extraordinary powers by framing his actions through the discourse of national security (ibid, p. 22). Agamben calls this unlimited power to control the economy of the nation, “a fact that is in perfect conformity with the already mentioned parallelism between military and economic emergencies that characterizes the politics of the twentieth century” (ibid). Again, during the Second World War, a similar claim to sovereign power was made, leading to the declaration of an unlimited state of emergency on May 27, 1941. This same rhetoric was used to suggest that Congress was unable to do what was necessary to protect the nation, allowing the president take the extreme measure of interning 70,000 US citizens of Japanese descent.

The increasingly slippery concept of national security, paired with geopolitical and technological changes to the nature of warfare in the second half of the 20th century, meant that military and domestic concerns were becoming increasingly inseparable. The creation and use of nuclear weapons changed the possibilities of warfare, prompting what Hannah Arendt calls “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, p. 6). This resulted in 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. Smythe notes that, until this point,“the proper function of the military [was] to “defend” the country against attack in order that the civilian sector may prosper in “peace.” The two types of activity [had] been assumed to be separate and distinct” (1986, p. 71), however, this idea is based on the “myth that the military arm can protect the civilian activity against disruption. While never true in reality, the coming of total mobilization in World Wars I and II, and the advent of nuclear weaponry, should have dramatically demolished the myth” (ibid, p. 74). 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 and Hanson, 2009, p. 2). The role of civilians grew even more important to military efforts due to the increasing reliance on research and development as the military struggled to come up with more intelligent and effective weapons to accommodate these shifts in warfare. This prepared the way for a dramatic expansion of the military-industrial complex, as Noble points out:

> [t]he notion of a “citizen army” greatly expanded the scope of the military activities which were now aimed at the preparation of the entire citizenry for possible military service: the new military creed, which identified training for industry with military training, coincided nicely with the corporate need for an “industrial army” of properly adjusted and assembled “economic units” (1977, p. 226).

The all-consuming national security imperative of the Cold War further collapsed any remaining distinctions between civilian and militarized spaces. National Security Council Resolution 68 (NSC-68)—possibly the most important doctrine of the Cold War—is referred to by James Chace and Caleb Carr as “the most forthright expression of... the universalization of threats to American security” (in Edwards 1996, p. 12). It stated that “a defeat of free institutions anywhere is a defeat everywhere” (ibid), thus expanding the national security prerogative and defining it in very ambiguous terms.

As a result of this collapsing of civilian and military domains, and the increasingly non-traditional format of national security threats, the need to protect the privately run critical infrastructure had become a focus during the Cold War. Emily Frye notes that “[p]rotecting the nation's roads, bridges, and telecommunication systems became a top priority when the possibility of massive and crippling physical damage resulting from nuclear attack, following the devastation evident at Hiroshima and Nagasaki, was clearly no longer a myth" (2002, p. 349). It is therefore unsurprising that one of the earliest focuses of cybersecurity was in terms of critical infrastructure (Dunn Cavelty 2008, p. 87). Since becoming connected to computer networks, these facilities have become vulnerable to attack, as they could be hacked into by outsiders and damaged. Because networked computing, and particularly the Internet, grew according to market demand after it left the purview of the military, it was developed without the same level of awareness of national security implications. In addition, the challenge that networked computing poses to "conventional ways of thinking about space, sovereignty, and security" (Saco, 1999, p. 262) due to its transgression of national borders, and the challenge that this in turn poses to state authority through the "blurring of traditional boundaries", prompted great anxiety from security advisers (ibid, p. 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, played into fears about asymmetric threats.

Therefore while the military had been wondering about the security of networked computing in warfare for some time, concern with cybersecurity was propelled onto the national agenda as a result of the information revolution in other areas of society. Networked computing had transformed rapidly from a handful of networks that were used mostly for defense research or operations at the beginning of the 1980s, to a civilian and commercial enterprise in the 1990s involving an enormous number of networks, and a much more practical and user-friendly system of organization following the creation of the world wide web (Abbate, 1999, p. 181). This resulted in the progressive automation and informationalization of businesses, industry, transportation, government, healthcare, and critical infrastructure, meaning that a system that had not been built with security in mind, was increasingly being used to store and communicate information that needed to be secure. While early understandings of network security outside of the military had been very technologically oriented and focused on the integrity and operability of the network, Hansen and Nissenbaum note that "it moved beyond a mere technical conception of computer security when proponents urged that threats arising from digital technologies could have devastating societal effects" (2009, p. 1155).

However Ralf Bendrath highlights a more self-serving motive for this concern, asserting that “[t]he [cybersecurity] debate started around 1990, when the Soviet Union collapsed and the threat-estimation professionals in the security community began looking for new ideas” (2003, p. 50). Barry Buzan, agrees with this assertion, noting that the end of the Cold War brought a ‘threat deficit,’ as the Soviet Union “for more than 40 years had created a common cause and a shared framing that underpinned US leadership of the West” (2006, p.1101). In the following years a scramble ensued to find a new enemy focus for US foreign policy. Despite the move away from total war owing to the possibility of nuclear warfare after World War II, it is clear that the system for modern war remained, including the military-industrial complex, military development of technology, and the centrality of war as a political tool for policy makers (Gray, 1997). Having lost their exterior enemy, the security professionals of the military-industrial complex had to find new threats to legitimize their existence. Gray argues that “[t]oday's international system of ongoing fear and tension is the *second* Cold War”, that it grew out of the first Cold War, and is “part of the same postmodern war system that has been in effect since 1945” (2004, p. xii, emphasis added). The events of September 11, 2001 provided a focus for the threat deficit, and allowed for the continuance of the postmodern war system Gray refers to. 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. David 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, p. 7).

The Global War on Terror would require a whole new set of weaponry and methods of defence. While foreign terrorists can be hunted out on their home soil, domestically-based terrorists require different tactics. As mentioned earlier, the necessity to pre-empt terrorist attacks is particularly great due to the ineffectiveness of punishment after the fact (Chandler, 2008). Increased surveillance and control of the Internet can therefore be understood as a way to combat the vulnerabilities introduced to critical infrastructures by connecting them to an insecure system which may be the target of non-traditional attacks in warfare. However it also mitigates the potential for the Internet to be a “staging ground for antisocial, disruptive, or dangerous organizations and communications” (Nissenbaum, 2005, p. 64). Therefore the unique features of cybersecurity seemed to fit well with existing concerns about asymmetric war and terrorist attacks. Bendrath notes that as concern with cybersecurity was popularized,

> it did not take very long until the highly technical problems of IT security—encryption, password protection, and intrusion-detection systems, to name but a few—were framed in terms previously known only from military policy. “Password security” became “computer security,” then “information-systems security,” “information protection,” and now “information warfare.” (2003, p. 50).

The next two decades witnessed a turf war over who would take responsibility for this burgeoning security industry and what ‘solutions' to security threats they would promote. The Air Force had long been a champion of cybersecurity, and had set up its Info War Centre shortly after the Gulf War in 1992, while the National Defense University graduated the first class of officers trained in cyberwar in 1995 (Clarke and Knake, 2010). The Pentagon's Strategic Command—also responsible for nuclear forces and Space Command—was given centralized responsibility for cyber war in 2002 but the Air Force's newly established Cyber Command would direct the war-fighting units. While the Air Force continued to assert its authority over cybersecurity, the Navy followed suit and formed its own cyberwarfare unit, and other Pentagon officials voiced concern over the Air Force's dominant role in the field. As a result, a multiservice Cyber Command was formed and opened its doors in October of 2009, and the Air Force Cyber Command became a numbered unit (ibid).

The intelligence community was also interested in taking responsibility for the security of cyberspace. The *National Strategy to Secure Cyberspace*, a component of the 9/11-inspired *National Strategy for Homeland Security*, charges the Department of Homeland Security (DHS) with the security of government networks and the coordination of national efforts to protect critical infrastructure. This has caused conflict with the National Security Agency (NSA), who some view as “the world's leading centre of cyberspace expertise” (Clarke and Knake, 2010, p. 37). Rather than attempting to replicate the NSA's skills in the U.S. Cyber Command, some have suggested that the NSA simply become the new Cyber Command (ibid). Director of National Intelligence and former NSA Director Michael McConnell is one such proponent. The DHS has voiced concerns about the increasing power of the NSA and the threat posed to the democratic process when one organization is responsible both for the security and monitoring all government networks, and foreign surveillance (ibid). In spite of these concerns, in 2010 General Keith Alexander assumed the joint role of Director of the NSA and Commander of the United States Cyber Command. This move has been questioned due to U.S. law which states that military operations should be governed by Title 10 of the U.S. code, and should be separate from intelligence operations which are governed by Title 50. Peter Singer has expressed concern about this move, noting that "[d]ouble-hatting the NSA and military Cyber Command has raised deep concerns about the militarization not just of cyberspace, but of an intelligence agency's core function of collection and analysis" (in Shachtman, 2010, para. 3).

The broadening of the scope of national security, and conflict over which government agencies should have jurisdiction in these new domains, has resulted in a messy and complicated turf war over the security of cyberspace, wherein national boundaries are increasingly difficult to enforce, and attribution is extremely difficult. The lack of clarity around jurisdiction in cyberspace, and the rhetorical power of 'national security' has allowed for some of the most egregious infringements on the freedoms of American citizens. Using what security expert Bruce Schneier (2008) has called "a terrifying piece of legal contortionism," George Bush in 2005 defended his authorization of a domestic warrantless surveillance program being carried out by the National Security Agency, by relying on his Constitutional powers and a joint resolution passed by Congress after 9/11 which led to the war in Iraq. This rationale suggests that "the president has unlimited powers to fight terrorism. He can spy on anyone, arrest anyone, and kidnap anyone and ship him to another country... merely on the suspicion that he *might* be a terrorist" (ibid, p. 26). When brought before court, an act of Congress granted retroactive immunity to the telecom companies involved in the warrantless wiretapping, while the government argued that the case should be barred as it could expose government secrets and undermine national security. Many believe the dragnet surveillance program continues today (Kravets, 2011).

Policy Window

This historical overview illustrates the central role that the military and the intelligence community have played both in the development of networked computing, and in the articulation of and response to developing concerns around the security of cyberspace. As Bendrath notes, “[t]he debate about national security in cyberspace... is not the only one about predicting the future, but also about how to prepare for it in the present; it is therefore highly political” (2003, p. 51). Different actors' predictions about future threats and how to combat them represent their divergent interests, and compete with each other for dominance. The history covered in this chapter facilitates the securitization of the computer security sector, framing information and communication technologies as part of a national cybersecurity concern. However the suggested responses to this threat are wide-ranging, and as Dunn Cavelty posits, not all problems or particular framings of problems are propelled onto the security agenda (2008). The winner in the battle to legitimize a certain response will be determined according to the social position of the actor, and their ability to effectively mobilize securitizing rhetoric and it is clear that the media’s role in agenda-setting could have a strong influence on this. As previously noted, John Kingdon's agenda-setting theory explores the conditions which allow for an issue or favoured response to be moved onto the security agenda; a moment which he terms a ‘policy window’ (in Dunn Cavelty, 2008 p. 33-34). He suggests that *indicators*, *formal and informal feedback*, and *focusing events* provide this window of opportunity. While these categories are not reasons themselves for an issue to be moved onto the security agenda, they can serve as focal points for debate around the type of response that is necessitated. These focal points attract media attention which functions as part of the agenda-setting process by mobilizing support for different threat frames and solutions.

Indicators

'Indicators', as opposed to 'events', are the result of investigations into the cyberthreat which confirm a problem and research possible solutions. One of the earliest 'indicators' that can be said to have garnered public attention for the issue of Internet security was the (non) event known as Y2K. As the year 2000 approached, the government, the private sector, and increasingly the public worried about the possibility that computers would be thrown into potentially terminal confusion when the twentieth century became the twenty first century. According to Emily Frye, concern mounted throughout the 1990s so that "[b]y 1997, concern about the so-called Y2K Bug had reached critical mass" (2002, p. 354). Y2K illustrated to the public, policymakers and industry leaders alike the extent to which Western society was dependent on networked computing, and the disastrous potential if the system ever failed. The media, in a frenzy of cyber-doom reporting, emphasized the inevitability of this outcome; for example Newsweek ran an article in June of 1997 with the headline, "The Day the World Shuts Down", in which they worried about everything from ATMs to weapons systems, and asserted that the U.S. government was not spending enough time or money working on a solution (Levy, 1997). François Debrix notes the centrality of the media in the production of the emergency culture that developed around Y2K:

> By hammering in the danger of the Y2K bug, multiplying scenarios of what would happen if, for instance, computers were to suddenly read 2000 as 1900... constantly running programs which were meant to provide the viewer with detailed checklists of what s/he needed to do in order to be Y2K ready, and updating everyone on how well government agencies were dealing with the anticipated glitches, the media made Y2K into a powerfully conditioning event.... In short, panic and emergency, fueled by the media, helped breed more uncertainty in the public about the entire Y2K phenomenon. The only thing that people soon became convinced of was that there were good reasons (because the media had said so) to be fearful and prepared. (2001, p. 152-153)

In addition, Frye notes that management efforts from public and private sectors "put cyberinfrastructure on the public-policy map" (Frye, 2002, p. 355), and although the potential of Y2K quickly faded from the public mind after the rollover to the year 2000 was successfully navigated without incident, it was not forgotten by policy makers. In fact Frye claims that the decision to form the President's Commission on Critical Infrastructure Protection (PCCIP) in 1996, was a result of concerns that Y2K might not be the only threat to cyberinfrastructure (ibid).

In the mid-1990s, at around the same time that Y2K fears were really starting to take hold, concerns in other areas of cybersecurity had also resulted in internal investigations to explore the risk and raise the alarm. These reports furthered the emphasis on computer security as an issue that should be dealt with by the government and the military. The first of these investigations occurred within military circles, where the importance of communications had long been acknowledged, but the centrality of the Internet to issues of national security was only just being conceptualized. As has been noted, the military separated its own sensitive networks from ARPANET, allowing the Internet to be developed and privatized. However as the Y2K scare proved, these privatized networks had become indispensable to many of the infrastructures upon which the nation depended, prompting a desire in some areas of the military to reassert military authority over the Internet. The formal launch of the concept of 'information warfare' occurred in 1992 with Department of Defense directive TS3600.1; however due to its classified nature, the implications of this new type of warfare on the public domain were largely unknown outside the military (Rattray, 2001). As part of this internal effort to explore the importance of and threat to cyberinfrastructure, Major General Frank B. Horton III asked RAND analysts Roger Molander and Peter Wilson to adapt their nuclear war simulations in order to portray a cyberthreat. The games were known as “Day After...” exercises in which various Defense Department officials played different roles as they attempted to defuse a crisis situation (Berkowitz, 2003). The “Day After... In Cyberspace” games would begin with a simulation of a traditional conflict such as a regional war, midway through which the situation would become complicated by a series of mysterious technological happenings, like the power grid suddenly failing, or a passenger train switching to the wrong tracks and ending up on a collision course with a freight train. The games were incredibly popular, but also concerning; defense officials began to realize they were unprepared for these kinds of attacks. As Berkowitz notes,

> The biggest problem was simply that you often did not know who the cyber attacker was. Sometimes you could not even tell an attack was underway. Did someone intentionally crash a computer to keep you confused? Or was it a normal system glitch? After all, everyone knew that computers were always crashing of their own accord. And, even if you think someone is screwing around with your computers, how do you respond? As one participating admiral said, “What am I supposed to do, nuke them for turning off our TVs?” (2003, p. 139)

The buzz around the “Day After” games spread throughout the military and began to reach the media, and in 1994, the first publicly available explanation of information warfare was released in the annual report of the Secretary of Defense (Rattray, 2001).

This was followed in 1996 by the Joint Chiefs of Staff report which gave a more comprehensive discussion of the public implications of information warfare, drawing the link between the dependance of the protection of military networks on the security of public networks. The report explained that, “the seamless relationship [between the US National Information Infrastructure and the Defence Information Infrastructure] makes distinguishing between them impossible. They share terrestrial telecommunications networks, a variety of information databases, and satellite communication networks. These infrastructures connect geographically separated forces and span international boundaries” (p. 2).

The other sector in which cybersecurity was developing as a focus was private industry, as the Internet was increasingly being used for commercial transactions, prompting concerns over the security of that information. However efforts to ensure personal security came into conflict with national security concerns over Internet security; a conflict that can be illustrated by what Diane Saco (1999) and Stephen Levy (1994) refer to as the 'cypto wars', or the tensions between government and software companies over the availability of encryption software. When Philip Zimmermann released his encryption program called Pretty Good Privacy (PGP) in 1991, he landed in hot water, as cryptographic devices in the 1990s fell under the definition of “Auxiliary Military Equipment”, and were therefore regulated by the International Traffic in Arms Regulations (ITAR) (Saco, 1999). By posting the software online and making it freely and globally downloadable, Zimmermann had unwittingly violated export restrictions on the distribution of 'arms' (ibid). The concern from within the government originated from the desire to ensure its ability to monitor foreign intelligence; an ability that was curbed by the use of encryption software. As a solution, the Clinton administration promoted the use of the 'Clipper Chip', a microchip used to scramble phone conversations that could be adapted for use in computers (a version of which the NSA developed, known as 'Capstone'). The messages or data can be decoded with the use of two wiretap 'keys' which are held in two separate locations 'in escrow' and are only obtainable by government entities by a warrant (ibid). Unsurprisingly, a solution to the encryption debate that involved the government being given a key to decode private data was unpopular, and received critical attention from the media. Saco notes that, “[i]nstead of the breachable 'privacy' that key-escrow programs offer, opponents favor the 'Pretty

Good Privacy' that Zimmerman's program promises and, by all accounts, delivers" (ibid, p. 271). As a result of this opposition, in 1995 the Clinton administration established a joint defense-civilian board that "pledged to accommodate a mix of commercial and federal methods for protecting electronic transactions" (in Saco, 1999, p. 282). New proposals had private entities holding a "commercial escrow", and offered export privileges to software companies who were willing to build wiretap escrow keys into their products (ibid).

Formal and Informal Feedback

Since the early 1990s, the U.S. government carried out various formal investigations into cybersecurity with the aim of persuading the major actors in cybersecurity—i.e. policymakers, industry leaders, and the public—of the need to develop a coherent policy. These policy documents consulted a range of actors, including industry representatives, military and government officials, and to a lesser extent, the general public and civil society groups. The first significant attempt at promoting awareness and acceptance of the cyberthreat was in a 1997 report written by the President's Commission on Critical Infrastructure Protection, called *Critical Foundations: Protecting America's Infrastructures*. It is on this report that the Clinton Administration's cybersecurity policy, *Presidential Decision Directive 63* (PDD 63) was based. The policy document is brief—only fifteen pages—which is in keeping with its position as a first attempt at articulating cybersecurity policy, however the *Critical Foundations* report was a much more in-depth exploration of the issues, as little was known or understood about cyberthreats, 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 the Bush Administration, 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, and the networking of critical infrastructure much greater, resulting in 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 was 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. The emphasis on the threat of terrorism and the emotive appeal to the public to fall in line with a national effort to improve national security through cybersecurity is clear throughout the document. 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. The most recent development to cybesecurity policy 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. Like the NSSC, it focuses on security holistically, including government, industry, and civilian networks. However both documents are conspicuously silent on the role of the military, despite being focused on national security and defence. They were written in very different political climates, and under different presidents who had very different expectations. The CPR gives little attention to a description of the vulnerabilities of cyberspace and the threat this poses to the nation, while the NSSC dedicates an entire section to the case for action. This different framing has two likely reasons; firstly, in the time that elapsed between the writing of the NSSC and the CPR, cybersecurity became an accepted priority issue that did not require justification. Secondly, former President Bush had a fairly low approval rating prior to the 9/11 attacks, and the onus was therefore on the administration to justify its every move. Conversely, Obama entered the presidency accompanied by an expectation of hope and change, and so the CPR was framed as an attempt to improve existing policy, not justify its existence in the first place. The NSSC was one of the first documents of this nature, suggesting new cooperation between industry, government, and the public to increase control over and therefore security of the national computer networks on which the country depends. By comparison, the CPR was dealing with currently existing partnerships, policies, and protocol, giving this document more of a bureaucratic management emphasis.

Focusing Events

While media coverage reflected the growing concern over the need for cybersecurity, and the debates over how to ensure it, much of the discussion has been purely hypothetical, resulting in a reliance on terms such as 'E-Pearl Harbour' and 'E-9/11', to tie the future threat to something more tangible. However in recent years, there have been several apparent manifestations of these scenarios that have served to bring the threat out of the realm of the hypothetical and into the real. In 2007 Estonia claimed to have been the victims of what was termed a ‘cyberattack’ that it claimed was waged by Russia. According to media reports, the attack was assumed to have been a response to the removal of a Soviet statue from the Estonian capital of Tallinn. Government websites, those of various political parties, banks and the media were targeted with Distributed Denial of Service (DDoS) attacks, which involves the flooding of a server with requests so as to overload it and render the sites it hosts inaccessible, in this case for weeks (Hughes, 2007, p. 2). In the following year, similar attacks against Georgia coincided with a physical invasion of the nation by Russian troops. The attacks were very similar in nature to those that had been carried out against Estonia; in the Georgian case the websites of the Ministry of Defence, Ministry of Foreign Affairs, various English language media, and Georgian President Mikheil Saakashvili, were taken offline by DDoS attacks. However in this case, the direct military action on the ground led media reports to reference the incident as the “world’s first cyberwar” (Portilho-Shrimpton, 2008, para. 1).

The realization of previously hypothetical cyberattacks struck closer to home in 2010, as search engine giant Google announced that it had been the victim of an attack that was traced to servers in China. Along with up to 34 other U.S. companies, Google's proprietary software had been targeted in an attempt at cyberespionage, and the Gmail accounts of several Chinese dissidents had also been compromised (Nakashima and Cha, 2010). This admission by Google marked a watershed moment for the regulation of the Internet for several reasons. Firstly, Google’s admission was a bold move which risked shaking public confidence in online information sharing by confirming the vulnerability of U.S. digital infrastructure and the private sector which relies upon it. Secondly, the attack prompted the unusual involvement of the government in the private sector, as the NSA was given access to Google's digital infrastructure to conduct an investigation (Nakashima, 2010a). And finally, the incident allowed the U.S. to challenge China’s Internet governance policies, shifting the framing of Google's fraught relationship with China from that of a commercial dispute, to one which was a concern for national security. This highlighted growing tensions between China and the U.S., and illustrated the increasing role which the ICT industry plays in international relations (Bremmer, 2010).

The attacks on Google were instrumental in bringing the reality of cyber-espionage to the attention of Americans, and highlighting the fact that private communications were targets in internal and also state-based conflicts. The attacks on Georgia and Estonia were important illustrations of the extent to which technologically dependent societies could be disrupted by fairly simple and low-cost attacks, although these were seen by many to be examples of mass disruption, not mass destruction. The way that these events were framed, drawing on the rhetoric of cybersecurity that had grown out of a long history of military involvement in technological research and development, facilitated the promotion of some security responses rather than others. The growing concern over the threat that computer-based attacks posed to national security emphasized the need for these responses without the necessary consideration of the impact they would have on civil liberties.

Chapter 4.

Method

Introduction

As has been explored, research suggests that the media can have an influence on the promotion of cybersecurizing rhetoric, and potentially on the development of cybersecurity policy. To explore this possibility, this study tracked the development of the discourse around 'cybersecurity' in the U.S. media, and examined the frames through which this issue is presented. While the expectation was that securitization will be a dominant frame as 'cybersecurity' has national security implications, due to the contested nature of this field there are several competing frames that are employed in reporting on cybersecurity. These include a computer security frame, a crime frame, a privacy and civil liberties frame, an anti-regulatory or free-market frame, and a public-private partnership frame. This study aimed to answer the following questions: Can a securitizing frame be identified in news reports on cybersecurity? Is this frame questioned? What other frames are used as an alternative to or in conjunction with the securitizing frame? This investigation did not address the ways in which computer security issues more generally are framed, as this is would necessitate the collection of an extremely broad data set that is beyond the scope of this thesis. Rather it verified the assumption that securitizing rhetoric is present in discussions of cybersecurity, and assessed how this frame is mobilized and changes over time.

In order to map the rise in the acceptance of the national security approach to networked computing in the media, two methods were used. In the first stage, content analysis was used to identify keywords based on existing cybersecurity literature that are understood to be indicators of a national security approach to computer security. These keywords were used to identify news articles on this topic, and to conduct a *content* *analysis* to indicate the popularization of these terms. Visually mapping the results of this analysis allowed for the identification of periods of increased focus on or interest in cybersecurity issues. The second part to this method involved a qualitative *framing analysis* of these periods of high concentration. The aim was to discover to what extent the chosen keywords are actually used to reference a securitizing frame, and whether these periods of increased coverage are indicative of events which may have influenced the development of the meaning of cybersecurity. My hypothesis was that the meanings of these keywords were discursively contested, but settled over time, and therefore while multiple frames may have been used initially, the eventual dominance of the securitizing frame indicated an acceptance within the media of computer security as a legitimate concern of national security organizations.

Part One: Content Analysis

I began by conducting a content analysis, using the databases *LexisNexis* and *ProQuest* to pull data from five of the U.S. newspapers with the widest circulation, so as to get a sense of dominant or popular frameworks. These included the *New York Times*, *Washington Post*, *Wall Street Journal*, *USA Today*, and the *Daily News (New York)*. The *Daily News* was included in place of the *Los Angeles Times*, which has a wider circulation, but whose archives were not fully accessible through the databases used for this project. Newspapers are not fully representative of how most Americans access news, and ideally a more comprehensive study would include an analysis of cybersecurity frameworks employed within major television networks, as well as alternative and online media sources. However this study is mainly interested in the circulation of dominant discourses, and research has shown that even in the digital age, traditional “brand name” news sources like *USA Today* and the *New York Times* are valued for their perceived authenticity, accountability, and autonomy (Hayes et. al, 2007). Studies show a high degree of convergence between traditional news sources and online alternatives like weblogs; Thomas Johnson and Barbara Kaye (2004) note that, while bloggers are often critical of traditional media, in order to present this critique they must pay attention to traditional media. Bloggers also often try to increase their credibility by citing traditional news sources, and similarly journalists often pay close attention to the 'blogosphere', and also host their own independent blogs. They also found that studies suggest Internet-based news supplements rather than replaces traditional news media (ibid). Of the news sources selected for this study, the *New York Times*, *Washington Post*, and *Wall Street Journal* are influential publications in Washington D.C., and therefore are likely to be more attuned to policy development as they are based close to the center of national government. John Kingdon notes in his research into policy agenda-setting that policymakers sometimes find it difficult to ensure that important information reaches Congressmen and senators due to the “oversupply of information,” but that “if the *Times* or *Post* picks up [a] report and does a story on it, they do read that, and it gets their attention” (1995, p.60). Therefore the relationship between these publications and policymakers is clearly important for an investigation of media effects in cybersecurity policy formation.

The choice of time period under examination was informed by the literature review, which identified a shift towards a distinct cybersecurity rhetoric in the 1990s. As Cavelty points out, concern with information and communication technologies dates back to at least the Second World War, however at this point ICTs were seen as ‘force enablers’ or ‘force multipliers’ (2008, p. 41). It was not until the 1980s when technological innovation resulted in the merging of telecommunications networks and computers, and the subsequent popularization of personal computers, that ICTs were conceptualized as possible vulnerabilities, or even targets for national security threats (ibid, p. 42). While an understanding of the central importance of ICTs is apparent in the literature, Ralph Bendrath asserts that a distinct rhetoric of ‘cybersecurity’ was not present until around 1990, “when the Soviet Union collapsed and the threat-estimation professionals in the security community began looking for new ideas” (2003, p. 50). Therefore the time period examined begins at 1990, and ends in 2010, which was the most recent complete year of data at the time of writing.

In order to identify a securitizing discourse as applied to computer security within these sources, and to produce data that was manageable in size and scope, a set of keywords were chosen—again informed by the literature review—which are representative of a framework of security that looks at ICTs through a national security lens; these are 'cybersecurity' and its various componants, 'cyberattack', 'cyberwar' and 'cyberterrorism' (including variations in spelling wherein the 'cyber' is hyphenated or exists as a separate word, for example 'cyber-security' and 'cyber security'). The prefix ‘cyber’ as a designation of computer-based function has become ubiquitous, as Burnett and Marshall note (2003). Originating in part in the *cyberspace* of William Gibson’s *Neuromancer* (1984), and also drawing on Norbert Wiener's theories of *cybernetics*, wherein information systems function using feedback loops which allow for constant adjustment according to changing circumstances, an array of neologisms have resulted (Burnett and Marshall 2003, p. 25). Of these, cyber*security*, cyber*attack*, cyber*war*, and cyber*terrorism* reference a range of traditional threats to the nation. The term ‘cybersecurity’ represents a broadened concept of 'security' which can be used to assess a wider range of potential threats to the nation. This is appropriate for a post-Cold War world in which total war is not an option, international conflicts are increasingly non-traditional, and a threat deficit created by the fall of the Soviet Union has resulted in a scramble to find a replacement enemy focus for US foreign and military policy (Buzan 2006; Gray 1997). It encompasses virtually all possible computer-based threats in a world where traditional notions of warfare and nationhood are constantly challenged. The inclusion of the more specific keywords 'cyberwar, 'cyberterrorism,' and 'cyberattack' allowed for an indication of which threats were of primary concern during different periods. However while these keywords represent very specific militarized threats which are posed by certain types of people in specific circumstances, their meanings are not static and their use can be flexible. They invoke the idea of security, but can be used in a range of circumstances.

In an initial search for data, the keyword ‘information warfare’ was included. This is a military term which was popularized early on in mainstream discussions of cybersecurity. It is used to refer to a range of strategies in warfare including propaganda, electronic warfare, targeting communications, misinformation, espionage, and both human and signals intelligence (Berkowitz, 2003). It was decided that its meaning is both too broad for the purposes of this study as it encompasses far more than networked computing, and at the same time is too narrow, as it originates from a specific lexicon of military strategy, rather than being a popularized neologism. This does not mean that ‘information warfare’ cannot be re-appropriated and used in similar circumstances as the other keywords, however it does not originate from the same cybersecurity discourse which began to circulate in both military, government, and the popular press in the

1990s; rather, it has been used to reference an established part of military strategy since at least the 1980s (Bendrath, 2003).

The keywords suggest which frame the reader should use to interpret pre-existing mental schemas, which contain pre-set understandings regarding consequences and responses (Fairclough, 1986). Therefore the chosen keywords reference general schemas with implied frames. This referencing is a common strategy of news media as it allows for a necessary reduction in the complexity of an issue, given the constraints of print space and airtime. However, condensing complex issues in this way does carry the risk that a term could be used incorrectly as it reduces an issue to its bare bones and presupposes prior knowledge of the origins of the term. Entman suggests that once a term has gained salience, the use of a new term might result in a lack of understanding or an issue being taken less seriously (1993). This could explain the unintentional (and in some cases intentional) flexibility and fluidity in the definition of the keywords which were sometimes used in what would appear to be inappropriate circumstances, as will be explored in the analysis. It was decided that the unit of analysis should be the articles in which the words were used as a whole, rather than the number of times the keywords appeared within the articles as, according to framing theories, “even a single unillustrated appearance of a notion in an obscure part of the text can be highly salient, if it comports with the existing schemata in a receiver’s belief systems” (Entman, 1993, p.53).

A comparison of the frequency of keyword usage across the specified time period was then used to illustrate the changing level of acceptance of and familiarity with the keywords, and the evolution of the salience of the threat. It was hypothesized that the different keywords would fluctuate in popularity year by year, influenced by external events which change the characterization of the threat. For example, it was expected that there would be an increase in usage of all keywords in the period directly preceding, and especially following, the attacks on the World Trade Centre in 2001. It was also expected that there would be an increase of the use of the term ‘cyberterrorism’ during this period relative to other keywords, as terrorism became the most salient threat-frame as a result of the attacks. In addition, a degree of overlap in terms of keyword usage within the individual articles was expected, potentially leading to an inflated estimation of keyword use, which is not something that would be indicated by a content analysis. For example, three of the four keywords might have been used in the same article, so this would count as three separate data points in the quantitative analysis, however they occurred within only one article.

Part Two: Framing Analysis

The second stage in this study involved a qualitative examination of a sample of the data retrieved. This examination was conducted to show whether the securitizing frame is present when these keywords are used, or if these words are used in conjunction with other frames. The ‘point’ of an article cannot be reduced to the ‘topic’; cybersecurity or networked computer security may be the topic, but the point involves the *meaning* that the reader is supposed to take from the article. The data compiled was too large to conduct a close reading on every article; therefore the second part of this analysis was conducted on one keyword only—'cybersecurity' as the primary keyword of concern—and on select years as determined by the data. The first and final years from which data was gathered were focused on so as to provide a comparison of the development of cybersecurity framing over time.

The analysis examined two features of discourse: frames and schemas. According to Norman Fairclough, a schema represents the elements that are covered when outlining a specific activity, for example in security there is that which is threatened, an aggressor, and proposed solutions. Frames tell us how we should feel about each of these elements, for example what national security means, who the aggressor is and what they have done in the past. Schemas therefore “act as cues for a particular frame, and the frame provides a place for each textualized detail within a coherent whole” (ibid, 80). In Copenhagen School terms, frames and schemas convey some of the facilitating conditions necessary for a successful securitization; the linguistic structure of the speech act constitutes the way that the issue is framed, while the wider socio-political context is represented by the schemas that are referenced. Fairclough notes that this method of discourse analysis examines both the meaning built into the structure of the text, and the influence on the interpretation of text that is exerted by an audience's relation to the author of the text, and any referenced 'experts', thereby illustrating the connections between language, power, and ideology. Therefore this analysis examined both “what's in the text and what's already 'in' the interpreter - that is, the common-sense assumptions and expectations of the interpreter” (1989, p.78). This necessitated an awareness of intertextual context, or the fact that the current discourse is connected to a series of previous discourses, and that this understanding “determine[s] what can be taken as given in the sense of part of common experience, what can be alluded to, disagreed with, and so on” (Fairclough 1989/2001, p.121). However an examination of audience members was beyond the scope of this thesis, therefore the analysis was limited to a discussion of the frames used and an awareness of the socio-political context in which they were communicated, rather than their interpretation by specific audiences.

There are several different schemas and corresponding frames that could be employed in the reporting of cybersecurity issues and events, and they will be outlined here in turn. Within *securitization*, the main framework of analysis, the three main components of a schema are the situations or ‘threat subjects’ which are presented as issues of security; who or what is threatened, also known as the ‘referent object’; and the ‘extreme measures’ or proposed solutions that are necessitated in order to mitigate the threat (Buzan et al 1998). The referent object is usually the nation, however the frame of national security allows for an expanded range of referent objects to those that are essential to the survival of the nation, for example critical infrastructure. According to the Copenhagen School, a threat must be 'existential,' however the national security frame allows for a broadening of the idea of 'survival' so that even a threat to the national economy or ideology could be understood to threaten the nation's very existence. The national security frame differs slightly depending on the nature of the threat subject. Understood by the Copenhagen School as an 'external facilitating condition' and by Fairclough as a 'schema', this could involve referencing objects that are generally perceived to be threatening (for example nuclear bombs or terrorist groups), or the comparison of the threat to past events that posed major threats (for example Pearl Harbour or 9/11). The way the issue is framed also shifts depending on the historical relationship that the U.S. has with the threat subject, which could be nation-states such as Russia and China, or a variety of non-state actors which are given a pre-existing history by invoking the amorphous schema of 'terrorism'. Depending on the threat subject and the referent object, the frame proposes different solutions. For example a threat posed by a nation state may require diplomatic maneuvering, or perhaps economic sanctions, or increased development and funding for U.S. defense in that particular area. A threat from a non-state actor, on the other hand, might require increased control, regulation or surveillance of a particular area, and often increased powers for defense organizations. The proposed solution may also be influenced by the securitizing actor who performs the security speech act, as different organizations vie for dominance in different areas of defense.

There were a number of alternative potential frames which were also used in articles concerning ‘cybersecurity.’ These frames show concern with the security of information, but the repercussions of the threat were different than within the securitization frame; the threat was not existential and does not result in cascading effects throughout society. The first of these is *computer security* which Helen Nissenbaum characterizes as being concerned with protecting computer systems against attacks which threaten the availability, integrity, and confidentiality of data and information networks (2005, p. 63). Therefore the 'threat subject' may not even be an attack, but rather the dependability or survivability of a system in the face of accidental failures (ibid). The 'referent object' does not include broader objects such as 'the nation' or 'society'; rather this frame focuses on the security of the system itself and the implications of a breach or failure on the individual users of that system, perhaps to the extent that businesses and organizations may be affected either directly or due to a lack of public confidence. The proposed solutions are therefore also very different; Ross Anderson suggests that this frame may portray computer security as “driven more by what customers want than by a mission to provide protection against objectively (or inter-subjectively) construed harm” (in Nissenbaum 2005, 65). By contrast the securitization frame goes beyond securing the private interests of stakeholders (at least rhetorically) and suggests a moral imperative to safeguard the public as a whole (ibid).

The *cybercrime* frame bears some strong similarities to the securitization frame, but differs in its characterization of the threat, and the proposed alternatives. The threat is not existential—though it may impact some isolated areas of society, it does not have a cascading effect throughout society. Because the threat is not existential, the proposed measures in response are unlikely to be extreme as they do not appear to be justified if the circumstances are not exigent and do not require a response beyond the realm of politics as usual (Buzan et al., 1998). Most instances of cybercrime are not obvious until they are discovered; they rely on their covert nature in order to continue being successful. While this is sometimes the case with issues of national security—for example espionage is similar in this respect—most widely publicized threats are assumed to result in a major event affecting the entire population. Some of the most commonly cited cybercrime concerns that are likely to elicit an emotive response similar to that of securitization are that of fraud, intellectual property theft, and online distribution of child pornography—incidents that clearly affect individuals (Nissenbaum 2005, p. 64). The importance of individuals as the ‘referent object’ is central in framing the threat as cybercrime rather than a national security concern. As Nissenbaum explains,

> [a] virus attack on the Internet that corrupts thousands of computer systems [could be] presented as a criminal attack *against thousands of individuals* and is the business of domestic law enforcement, constrained by relevant protocols of investigation, arrest, and so forth. This same attack, within the cyber-security model, may be construed as an attack *against the nation*, and count as evidence for securitization. (2005, p. 72, emphasis added)

However in some cases the cybercrime frame can overlap with the securitization frame as economic impacts have begun to be discussed in national security terms, and the 'damage' caused by a cyberattack is often measured in economic terms in both frames. Similarly, specific types of cybercrime (for example those involving distributed denial of service attacks) are increasingly absorbed into a national security frame as some nation-states are known to 'sponsor' attacks that are carried out by criminal or independent organizations so as to ensure deniability (Van Eeten and Bauer, 2009).

It is often suggested that *privacy and civil liberties* need to be balanced with security, or that one must be traded for the other, and so such a frame is often at odds with various security frames. Jennifer Chandler highlights the paradox that “security measures intended to protect a liberal democracy can end up eroding the civil liberties at the heart of that liberal democracy” (2008, p. 121). This frame is almost the reverse of a national security frame; where securitization equates government and the populace as 'the nation', the privacy and civil liberties frame divorces them and focuses on the populace and sometimes marginalized groups as the 'referent object'. The 'threat subject' is therefore government regulation, and the threat comes from the government or law enforcers themselves. Such a frame therefore questions the effectiveness of security measures, and asks whether a less privacy-invasive method could be used to the same effect, whether the benefits to security are worth the costs to privacy, and whether the privacy of certain people is more adversely affected than others (ibid, p. 122). The motives of the government and security institutions are often called into question, and the securitization frame is critically engaged with. Given this critical approach, and the suggestion that privacy and security are on opposite poles, the privacy and civil liberties frame is not often seen alongside a securitizing frame, as securitization emphasizes the urgency of the situation in order to promote security above all other concerns.

However the civil liberties frame does sometimes complement an *anti-regulatory or free-market* frame, which focuses on the positive effects of a free and open Internet, especially to a growing economy, and questions whether government regulation and cybersecurity measures might negatively impact business (Saco, 1999, p. 266). The anti-regulatory frame emphasizes the private sector's mistrust of government regulation (Clarke and Knake, 2010) and questions the state's need to assume a mediating role to manage the use of the new technologies (Saco, 1999, p. 273). It is similar to the civil liberties frame in that it takes government regulation as the threat subject and poses industry, the consumer, and by extension the nation, as the referent object. In this way it is sometimes possible for a free-market frame to suggest that national security moves are damaging to the economic security of the nation. In the case of cybersecurity is can be suggested that the state's policy "is causing [industry] to lose international sales to foreign competitors unconstrained by similar restrictions" (ibid, p. 270).

The *public-private partnership* frame is very similar to the anti-regulatory frame as it focuses on the importance of industry and the economy, and supports a free-market approach. However in this frame the government is not a threat to this approach; rather is seeks to foster innovation and economic development while also promoting security by partnering with industry. Due to the increasingly transnational nature of industry and corporations this frame may similarly emphasize the global nature of the Internet and the need for the government to enforce international regulation or to conduct foreign policy with the best interests of national industry in mind. The government does not regulate industry, but works alongside it towards a common goal. This idealistic frame mirrors the relationship fostered by the military-industrial complex, however it is dependent upon the belief that government and industry's goals can always be in line with one another.

News articles do not always follow so crude an outline; the choice over how to frame a news event often results in a more complex telling. However as Fairclough notes, the framing of a news report may be what is remembered by an audience, as “once we identify a text as an instance of a pattern, we happily dispense with the mass of its detail and reduce it to the skeletal shape of the familiar pattern for purposes of longer-term memory and recall” (1986, p. 160). Furthermore, he suggests that “aspects of events which do not conventionally get separated out as structural elements, will tend to disappear from view and consciousness” (ibid, p. 138-139). Therefore information that does not fit within a frame may not achieve the same degree of salience with an audience. In addition, Kahneman and Tversky demonstrated that “frames select and call attention to particular aspects of the reality described. This logically means that frames simultaneously direct attention away from other aspects” (Entman, 1993, p.54), and so a frame may actively discourage consciousness of information that does not fit within it, even if it is mentioned in the article. An analysis of the frames employed therefore took note of which frames were used in the article, the frame that was dominant, and the frame that was most often employed over time.

Case Study: Google vs. China

A media framing analysis of the 'cybersecurity' data allowed for conclusions to be drawn about the way this sector is discussed in the media, and how this changes over time. It illustrated the prevalence of a securitizing discourse, and how often the dominant news sources questioned the official framing of an incident. It highlighted any differences in the way different events are framed, and while it did not show causality, suggestions can be made as to why events were framed in this way. The method of data gathering limited this analysis owing to the securitizing bias of the keywords used for the content analysis. Therefore it focused on the use of the frame, and did not accurately reflect how the frame was mobilized and how issues were discursively fought over. Therefore this analysis was supplemented by a secondary qualitative analysis of a case study of a cybersecurity event, the selection of which was informed by the analysis of the 'cybersecurity' data set: cyberattacks originating in China and targeting search engine giant Google received a proportionately high level of media coverage in 2010 (43 articles out of the total 233), suggesting that it was a significant cybersecurity event. A second set of data was gathered using the same method and the same sources as were used in the first data set collection in order to ensure the inclusion of all alternative frameworks and avoid a securitizing bias. The keywords used to gather this data set were “Google” and “China”, with the search parameters being limited to the year 2010. The data were sorted manually to ensure that the cyberattacks were mentioned in the articles, rather than another incident involving these two actors. The framing of the event in this case study was analyzed to establish the dominant framing that was used. An analysis of the treatment of a specific cybersecurity event allowed for a better understanding of the effectiveness of the securitizing frame, both in terms of its ability to trump alternative frames, and in terms of its ability to facilitate the promotion of cybersecurity policy developments.

Chapter 5.

An Analysis of Competing Media Frames

This chapter will present the findings in the analysis of the frames used in news reports on cybersecurity issues. It will first present the results of the content analysis, examining the shifts in the use of this framing over time, and the external 'facilitating conditions' that may have influenced the choice in framing during different periods. Then the results of the qualitative framing analysis will be presented which will examine the internal facilitating conditions that support or question the securitizing move. This analysis will focus on the data relating to the 'cybersecurity' keyword during 2010, and the spikes in usage will be looked at more closely in order to get a clearer idea of the way issues are framed and why this might be.

Part One: Content Analysis

A total of 2205 articles were gathered using the search terms—referred to here as *keywords*—'cybersecurity,' 'cyberattack,' 'cyberwar,' and 'cyberterrorism' and searching five news sources between January 1990 and December 2010. There was some overlap as multiple keywords were used within the same article, however as illustrations of the popularity or commonality of the keywords, it was important to count each occurrence as a discrete piece of data regardless of whether the article contained more than one keyword, and regardless of how many times that keyword appeared in the article itself. The term 'cybersecurity' was the most commonly used, appearing at least once in 1052 articles. 'Cyberattack' was the next most common with 746 articles, followed by 'cyberterrorism' at 245, and 'cyberwar' at 162. In what follows the periods and frequency in which these keywords appeared will be analyzed to highlight patterns, and to formulate hypotheses about the reasons behind these fluctuations. The results of the initial quantitative analysis are displayed in Figure 1 below.

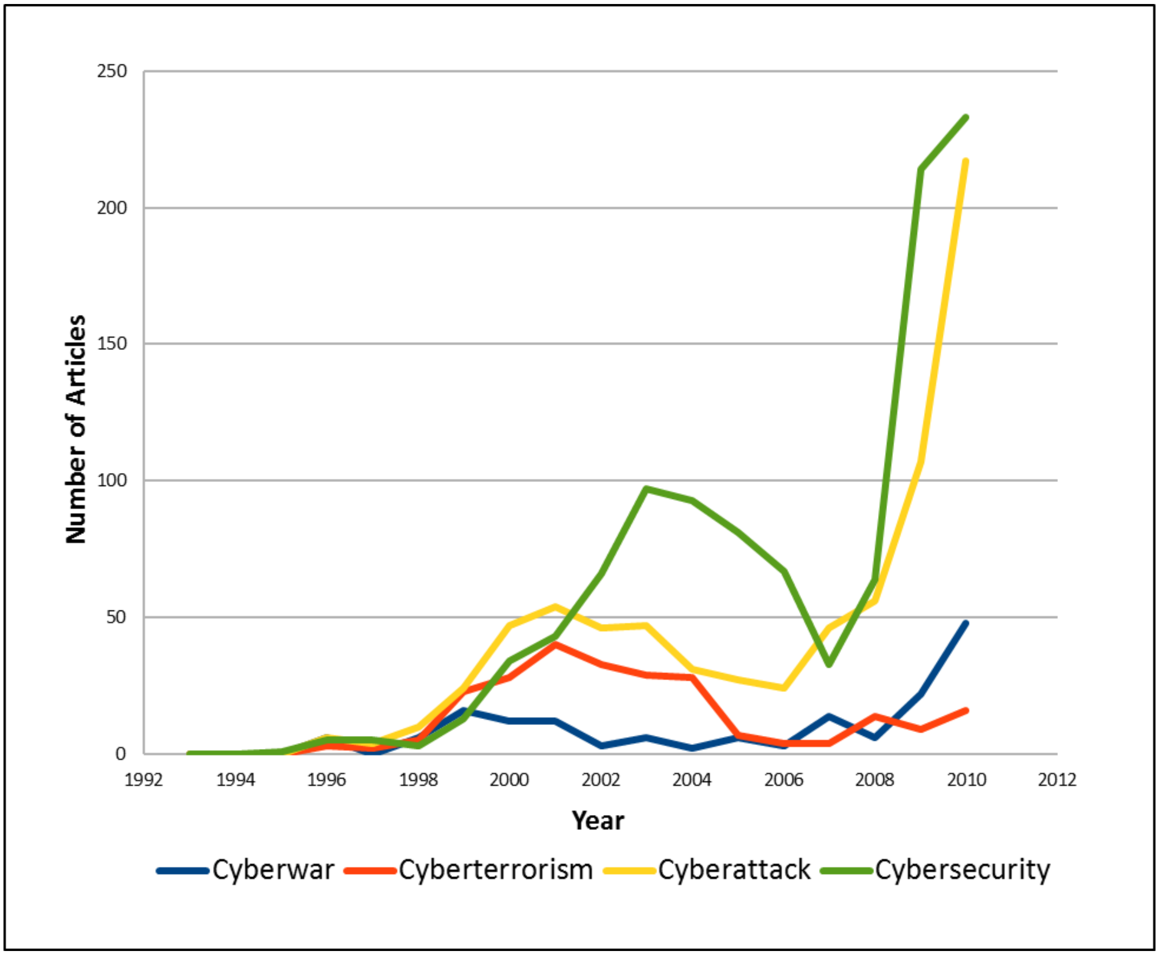

Figure 1. Number of Articles Referencing Keywords 1990-2010

As the graph indicates, the first usage of any of the keywords was in 1995, which suggests little public awareness of these issues prior to this, or that the hypothetical threat was not considered particularly newsworthy. However this does not mean that the issues referenced by the keywords were not being discussed prior to this; different terminology may have been used, for example the military term 'information warfare', or much less specific terminology such as 'computer security'.

The general increase between 1990 and 2010 could simply be due to the fact that more people own computers and more of the nation’s infrastructure relies on networked computing, meaning that it is a more familiar concept. It could also be that since the term has become more familiar a greater range of events are being described as issues of cybersecurity; for example internet-based crime, online smear campaigns, website defacement etc. Or it could be the case that greater focus is being given to computer-related events which impact national security as a result of an increased awareness and acceptance of the threat. The year 1995 was mid-way through the Clinton administration's first term, and was the year before President Clinton formed the Presidents Commission on Critical Infrastructure Protection (PCCIP) which was tasked with formulating a national security strategy to protect critical infrastructure against cyber attacks. The growing awareness among security professionals of computer-based threats that prompted the first steps in policy creation and official response therefore coincides with the beginnings of public awareness of these issues.

The keywords all begin with low level usage over the first few years. The 'cybersecurity' line begins to steadily increase after 1998, increasing sharply after 2001 and peaking in 2003. The high activity around this time is likely owing to the attack on the World Trade Centre in 2001, resulting in a sudden and heightened awareness of security threats of all kinds. This peak of media awareness coincides again with the development of new cybersecurity policy, as President Bush's National Strategy to Secure Cyberspace was released as a component of the larger National Strategy for Homeland Security in 2003. After 2004, occurrences of the keyword 'cybersecurity' decline, dropping off sharply between 2004 and 2007, before rising again and suddenly increasing in 2009 and continuing upward in 2010. The rise following the World Trade Centre attacks in 2001 could be part of an expected general increase in security awareness following a major domestic security incident. However there is no corresponding national security incident 2009 or 2010 on the same scale that could account for the massive increase in usage of the 'cybersecurity' keyword. Therefore it is likely that any incident resulting in this increased focus would be an occurrence that is specifically related to networked computer security. It is also likely that such an incident would have occurred in conjunction with a conscious attempt to carry out a securitizing move; as we have established, the media has a short attention span, meaning that newsworthy events are covered and quickly replaced by new occurrences, so this level of usage is unlikely to have occurred due to the coverage of a single event. Therefore this sustained and increasing usage of the keyword suggests an effort by security professionals to maintain public focus on the issue.

The 'cyberattack' keyword mirrors the development of 'cybersecurity' until 2001, although the numbers are slightly higher, perhaps indicating a connection between understandings of security as being related to attacks, either defensive or offensive. This relationship seems to decrease between 2001 and 2006, as 'cyberattack' drops off in usage while 'security' continues to rise and then declines much later, after 2003. This could be explained by the socio-political climate following the World Trade Centre attacks; the 'attacks' themselves were fleeting, whereas the response was a steady increase in 'security' efforts so as to prevent any future attack. From 2008 'cyberattack' parallels 'security' again, but the numbers for 'security' are now above 'attack', and both increase dramatically in 2009-2010.

The 'cyberterrorism' keyword also mirrors the development in usage of 'security' and 'attack' up to 2001 which is, unsurprisingly, its high point, coinciding with the 9/11 attacks and the subsequent focus on terrorism. Perhaps surprisingly, however, it begins to decline after this rather than indicating a sustained media focus on terrorism relating to networked computing, and rises only slightly again in 2003, perhaps as a result of the policy development around this time. After 2004 it drops suddenly and stays close to the baseline, with a slight rise in 2008 and 2010, perhaps reflecting the reporting of specific incidents.

The 'cyberwar' keyword follows the same pattern as the other keywords initially, but only rises until 1999, dropping off again rather than continuing to rise until 2001 as the other keywords do. Rather it decreases steadily to 2002, perhaps as terrorism became rhetorically established as the main challenge to security and nation-states became less of a focus. 'Cyberwar' remains close to the baseline until 2007, when there is a slight increase and subsequent drop, as if in response to a specific incident—perhaps the so-called cyberwar between Georgia and Russia that occurred at this time—however it then increases steadily to 2010, perhaps as part of the securitizing move indicated by the increase that can also be seen in the use of 'cybersecurity' and 'cyberattack'.

However to assess the level of acceptance within the media that is indicated by the increased use of these keywords it is necessary to look more closely at the articles themselves. This data merely indicates that the terms themselves were being used and therefore have increased in familiarity, but the context in which they appear could be critical of their usage, or of the actions that the terms are used to reference. Acceptance of the terminology does not indicate acceptance of the securitizing frame itself. However there is not space in this thesis to carry out a detailed analysis of all the articles; therefore the results of the content analysis will be used to isolate periods of interest upon which a qualitative analysis can be conducted. While all the keywords evoke national security schemata, 'cybersecurity' and 'cyberattack' are the most flexible in their definition and could therefore be applied to a wider range of phenomena. It is likely that these words could be used as well as, or even in place of the terms 'cyberwar' and 'cybterterrorism'. The graph in Figure 1 indicates that 'cybersecurity' also demonstrates the highest growth and most radical change over the period under examination. Therefore in the interest of time and given the focus of this thesis on security discourse, further investigation will be limited to the term ‘cybersecurity’. Figure 1 also indicates that 2010 was the year in which the keyword was used in the highest frequency and would therefore be an important year to examine. While 2009 experienced the largest shift in usage of the term, in 2010 the frequency of usage continues to increase, suggesting something more than a response to a specific event, but rather the acceptance of an ongoing agenda-setting effort. This analysis will assess the validity of this hypothesis, questioning what caused this shift and whether it is an indicator of a rise in popularity and acceptance of the term. In order to provide a point of comparison for the coverage in 2010 a qualitative analysis will also be conducted on the years 1995 and 1996, when the first instances of keyword usage were recorded. This will give some context for the spike in usage of cybersecurity terminology and establish whether the frameworks through which these issues are portrayed have shifted over time.

Part 2: Framing Analysis

'Cybersecurity' Framing During 1995 and 1996

Usage of the keyword 'cybersecurity' is fairly low between 1995 and 1996, with only six articles in total using the term. The first usage comes at the end of 1995, so the decision was made to also include the articles from 1996 in order to have a wider sample to draw from in making a comparison to later uses of the term. Figure 2 below indicates the distribution and frequency of the articles containing the keyword during these two years.

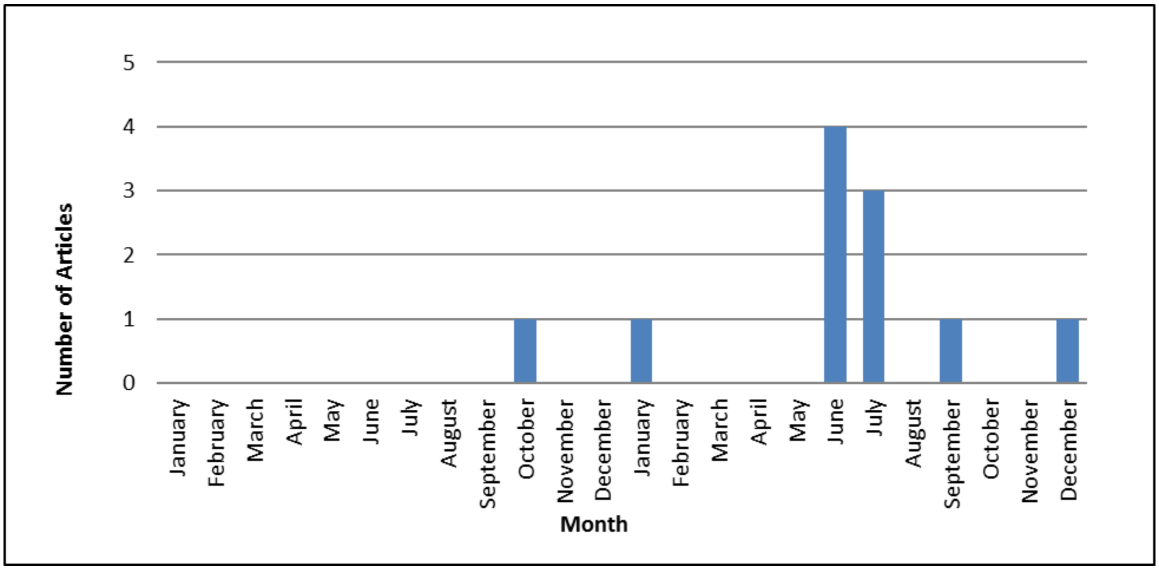

Figure 2. Cybersecurity Reporting Between 1995 and 1996

The first mentions of cybersecurity in 1995 and 1996 illustrate a conflict of two clearly defined frameworks wrestling for dominance; the *free-market* or *anti-regulatory* frame which focuses on the importance of economic progress, and the *national security* frame which promotes the importance of regulation. In the first article that mentions cybersecurity—in October of 1995—the 'topic' is the 'Clipper Chip'; a proposed encryption method for which the government would have a key, and which would be the only method of encryption allowed for computer communications in the U.S. The 'point' or dominant frame is the *free-market* frame, although others are also present. It is an editorial that is highly critical of government regulation which purports to increase cybersecurity while having the side effect of limiting the economy. ‘Cybersecurity’ in this article is defined as the degree to which the Internet is “safe for business” (USA Today, 1995, para. 1), something which would be achieved through powerful encryption. However such encryption was “blocked by government export regulations that make the programs difficult if not impossible to market, even for domestic purposes” (ibid, para. 4). Government regulation is clearly framed as the antithesis of successful business; is it proclaimed to be “not right” and moreover, “not necessary” (ibid, para. 5, 6). There is a strong emphasis on self-determination and the rights of individuals to protect their property which overrides government concern with national security. Alongside the *anti-regulatory* frame, a *civil liberties* frame is also invoked to describe the government-proposed solution involving the distribution of powerful encryption to which the government would have a ‘key’. This solution would override a “citizen's right to be free from government monitoring” (ibid, para. 9) and is “vulnerable to abuse” (ibid, para. 10). The events at Waco and Ruby Ridge invoke schemata that emphasize distrust of the federal government (ibid, para. 11).

An article using the same frames appears in December of 1996 covering the same issue, however the emphasis is slightly different according to which frames are given the most weight. The government is portrayed as behaving in an underhand manner, as it “sold the rules [that limit encryption exports] to the industry this fall as a liberalization of such exports. But in the writing, the administration bowed to demands of law enforcement and security officials” (USA Today, 1996, para. 8). This also suggests that the government did not act in the best interests of businesses and the “legitimate customers of the U.S. software and computer industry” (ibid, para. 11). The *civil liberties* frame is stronger in this article, as the title itself proclaims that “Privacy takes another hit from new computer rules”, suggesting that regulation is primarily damaging citizens’ right to privacy. Later in the article, it is stated that encryption is “free speech”, again emphasizing the underhandedness and perhaps unconstitutionality of government regulations (ibid, para. 10).

The other articles in 1996 promote the alternative frame of *national security*. The 'topic' of these articles is the development of a cybersecurity strategy, which seems to be related to the report generated by the President's Commission for Critical Infrastructure Protection and the resultant Presidential Decision Directive 63. Government attempts to secure the Internet are not portrayed as regulation that pre-emptively controls, but rather that is a necessary response to attacks by adapting existing legal systems to the new challenges of cyberspace. The securitizing frame is strongly supported; the title of one article proclaims that the cybersecurity plan is “urgent,” a connection is drawn in the first paragraph between the necessity of securing cyberspace and the need for an atomic bomb program in World War Two (Zuckerman, 1996a, para. 1), and the article compares a cyberattack to the attack on Pearl Harbour (ibid, para. 20). Another article makes a comparison to the Oklahoma city bombings (Zuckerman, 1996b, para. 5), and another puts a cyberattack on par with a Unabomber (Zuckerman, 1996c, para. 5). Potential aggressors are identified as “terrorists or foreign attacks” (Zuckerman, 1996b, para. 3) and the referent object is the nation’s critical infrastructure—for example the power grid, transportation, and financial services—without which the country could not function. The articles are based around the testimonies of various security officials and members of government, for example the Deputy Secretary of Defense, the Attorney General and her deputy, various senators, and CIA General Council. Each article opens by noting that these actions are being taken by the Clinton Administration, and are therefore fully endorsed by the President. This reliance on official discourse is typical of both the securitization framework and of news reporting, and it adds legitimacy to an uncritical reporting of government actions.

The second frame that is clearly present in these articles is that of *public-private partnership*. One article states in the title, “Clinton administration sees role for both public, private sectors on new commission” (Zuckerman, 1996a) and emphasizes that a cybersecurity strategy would be a “cooperative venture” (ibid, para. 7) with the private sector based on “trust” (ibid, para. 8), and that the private sector role is “critical” (ibid, para. 8). This frame complements the *securitization* frame, which is unsurprising given its reflection of the relationship between security and industry that was central to the military-industrial complex. However the frame that is conspicuously absent is that of civil liberties; for example the legal protections prohibiting CIA involvement in domestic investigations are referred to as “turf disputes” (Zuckerman, 1996a, para. 12) which merely complicate government efforts to secure cyberspace, rather than being necessary restrictions on the jurisdiction and power of the intelligence community. While the *civil liberties* frame appears with the articles whose focus is *anti-regulatory*, it is largely incompatible with the *national security* frame.

From these examples, it is clear that *anti-regulation* and *civil liberties* frameworks are invoked when government regulation negatively impacts industry. However when a framework of *public-private partnership* is used, *national security* frameworks are much more positively portrayed in the press and civil liberties are less likely to be of concern. The connection between government actions and policy development is also apparent; the 'topic' of the articles is either the development of cybersecurity policy, or the impact that government decisions around cybersecurity are having on the public sector. This indicates that the public perception of cybersecurity is being driven by policy initiatives, and therefore suggests that those articles with a *national security* frame may be part of government efforts to perform a securitizing move towards computer security. The presence of frames which question this approach, promoting considerations of civil liberties or taking an anti-regulatory stance, suggest that this securitizing move has not yet been successful, perhaps because ideas of cybersecurity are new and the threat has not gained enough salience to be fully accepted.

'Cybersecurity' Framing During 2010

By 2010, there are 233 articles which use the term ‘cybersecurity’, a dramatic increase from a total of 6 between 1995 and 1996, that indicates a much greater awareness of the issue. To investigate my hypothesis that greater focus is being given to computer-related events which impact national security, it is helpful to look at the pattern of usage of ‘cybersecurity’ during 2010. The graph in Figure 3 below shows a major spike in January (when the Chinese cyberattacks on search engine Google were announced), followed by a drop to a more consistent level of usage thereafter. However this consistent level is still high with an average of 19 articles per month mentioning 'cybersecurity'—an average that only reduces to 18 when the spike in January is excluded, illustrating a relatively high awareness of the issue throughout the year.

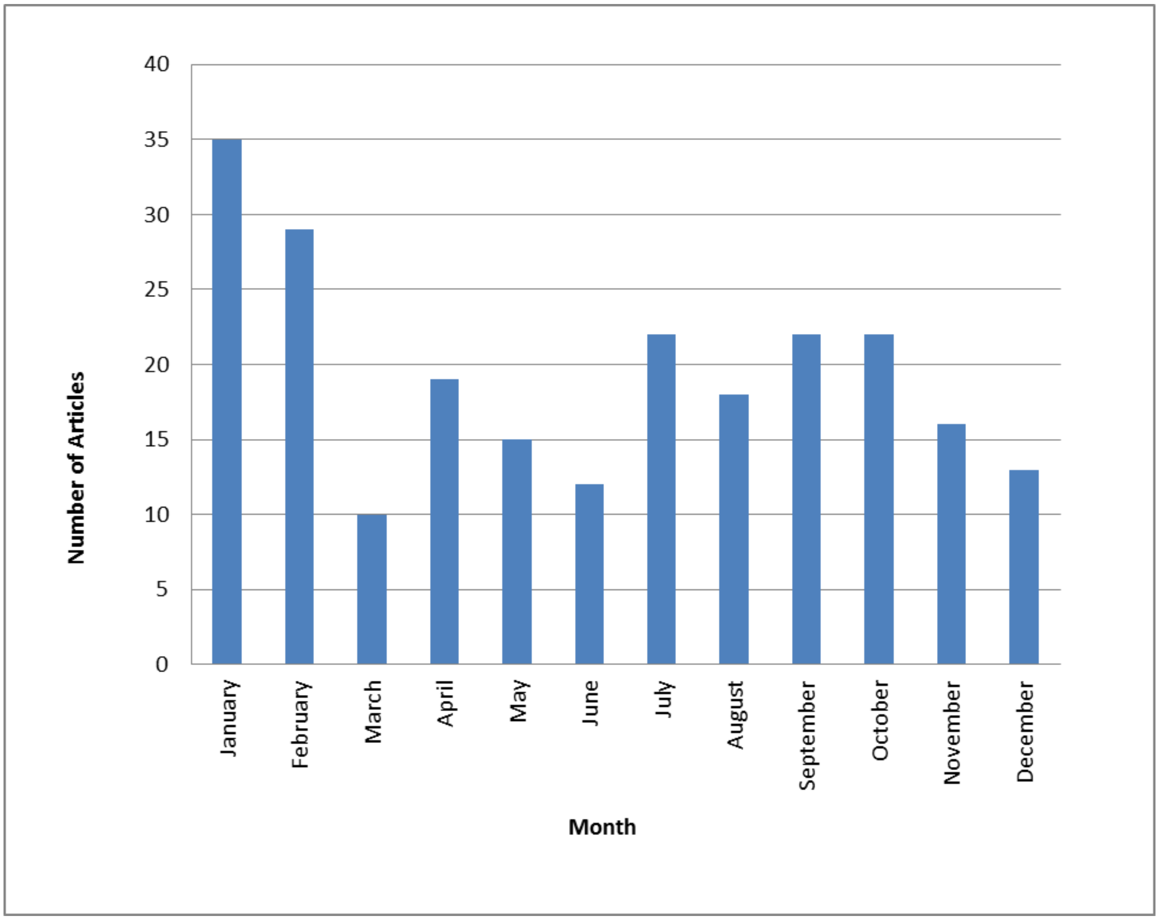

Figure 3. Frequency of ‘Cybersecurity’ Usage in 2010 by Month

The first step of a closer examination must differentiate the 'topic' of the articles from the 'point', which is indicated by the frame and schemata that are mobilized. The term 'cybersecurity' is used in a range of situations or 'topics'; the data reveals nine different categories of article, with some overlap between them. The first category includes 53 articles in which cybersecurity is referenced as part of a name or title, for example in weekly listings of museum exhibits or television shows. This indicates the growing popularity of the term and significance of the field, but does not really contribute to an understanding of the framing, and therefore will be excluded from further analysis. A second category involves articles on computer-related crime, and a third, technical issues with specific computer systems. The remaining groups are much more clearly related to national security. The fourth topic is the institutionalization of computer security, whereby military or intelligence organizations are given increased authority in these areas. Foreign policy and international relations concerning cybersecurity constitutes a fifth category. A sixth set of articles focus on the education or training of cybersecurity-related personnel, usually within traditional security-based institutions such as the military. A seventh set features specific events or attacks on the information infrastructure. Policy developments and new regulation make up the eighth group, and finally independent and government-commissioned reports on cybersecurity developments are also reported on.

These findings suggest that there is a greater awareness of and investment in networked computing in 2010 as compared to 1995, and that a wide range of issues is being included under the banner of 'cybersecurity'—for example cybercrime and technical issues with individual systems. However the majority of articles have a strong national security connection, suggesting that 'cybersecurity' has become an accepted concern of national security. There are a substantial number of articles (52) that do not focus on cybersecurity as the main topic, but rather contain broader discussions of national security issues and their relation to developments within industry; for example developments in defense contracts with Northrop Gruman including those in the area of cybersecurity, or a company's maneuvering to become a bigger player in this field, or government investment in research and development that included cybersecurity. These articles often used a securitizing frame, however cybersecurity was not the main focus. This highlights the strong connection between national security and industry that is reflected in the framing of some of the other articles.

Of the remaining articles in which cybersecurity was the central topic, 58 clearly demonstrated the securitizing frame while 53 emphasized the importance of public-private partnerships. These two frames were used together almost 50% of the time, emphasizing the strong connection between public-private collaboration and national security. In comparison to the articles from 1995 and 1996, it is clear that this has become the dominant pairing; appearances of the securitizing and public-private frames account for over half of the total identified frames in 2010. Computer security and cybercrime tended to be used discretely, with 13 of the 18 articles that focused on crime framing cybersecurity in terms of crime alone, and 7 out of 8 articles that focused on computer security framing cybersecurity as an issue only of computer security. Conversely, the anti-regulatory frame is only used alone in 3 out of the 9 articles in which it appears. This would seem to indicate that the definition of the term 'cybersecurity' is still contested to a certain extent, however the meaning or 'point' is converging on a dominant understanding that involves national security and industry, while other definitions involving technical or criminal understandings are used separately and less often.

However the most interesting shift is in the framing of privacy and civil liberties; 26 articles invoked a civil liberties or privacy frame and of these only 6 articles focused exclusively on privacy issues. In contrast to the articles from 1995 and 1996, a civil liberties frame was often paired with a securitizing frame, and these were not always placed in opposition. These frames appeared together in 10 of the 26 articles, including some overlap with a combination of public-private and civil liberties frames, which appeared together in 13 articles. The combination of a civil liberties frame with securitization and a public-private frame highlights a different meaning of cybersecurity to that emphasized in 1995 and 1996, when the media voiced concern over government interference with industry. Instead, these articles seem to emphasize the role of the government in protecting civil liberties online, and the benefits this freedom brings to private industry.

This new combination of frames is seen most frequently in articles which discuss the topic of an incident that occurred between China and search engine giant Google. The majority of these articles were published in January, accounting for the spike seen in Figure 3. A total of 43 articles in the 2010 sample either have this incident as their main topic or make reference to the incident, indicating that it has been incorporated as a referent object into a schema for which the corresponding frame is securitization. This may influence the framing of future cybersecurity discussions even though this incident is not the central topic. Fairclough (1989) highlights the significance of schemas in critical discourse analysis as, while a frame may not appear in a particular article, the referencing of a schema may connect the text to a frame that was promoted elsewhere, if the framing has been consistent. As Figure 4 below illustrates, the frequency with which the incident was reported on in the data set is lower than the overall number of articles but mirrors the pattern of reporting on cybersecurity issues at least until June. This suggests that the incident had a longterm impact in the way that cybersecurity was framed.

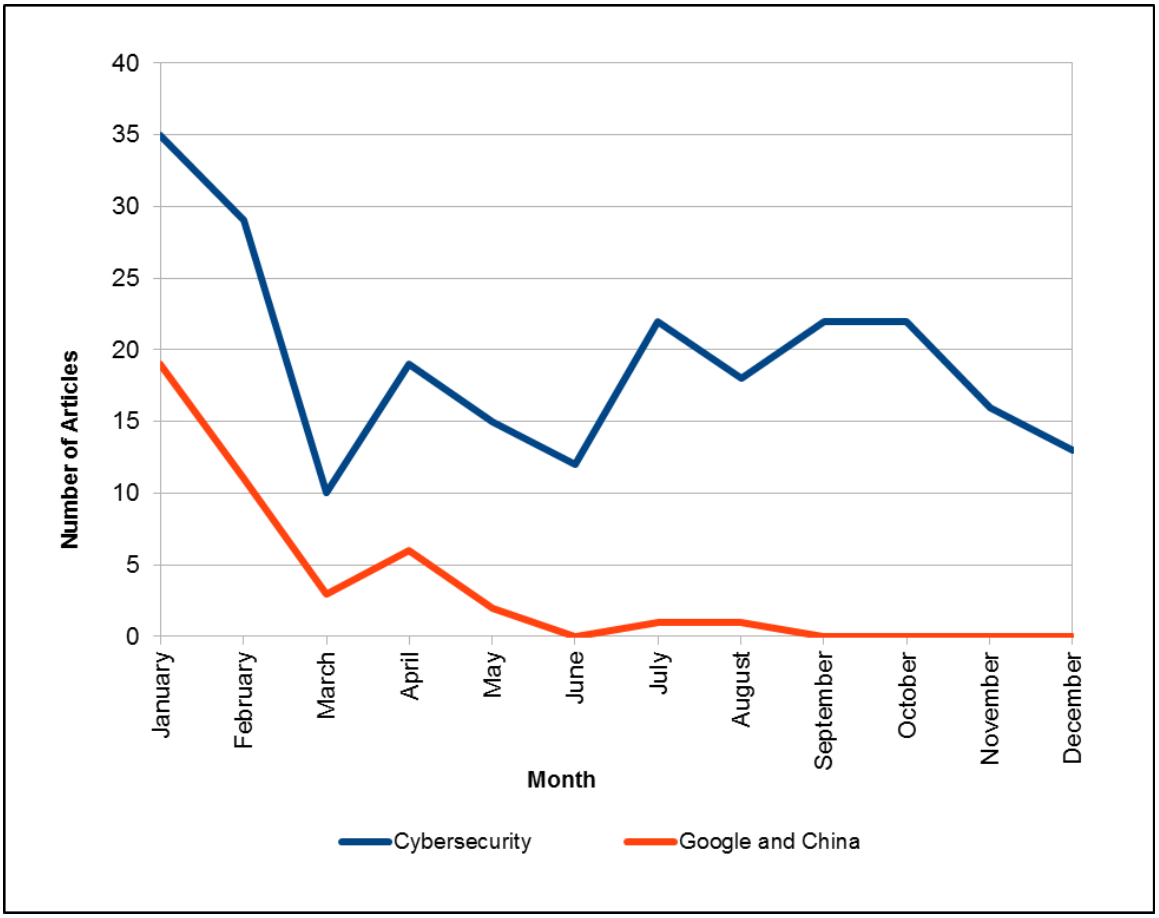

Figure 4. ***'Cybersecurity Usage in 2010 Compared to 'Google' and 'China'***

Note. Frequency of keyword 'cybersecurity' usage in 2010 by month was compared with the number of these articles that also reference the Google-China incident.

The incident involved the breaching of Google's digital infrastructure, and that of as many as 34 other major U.S. companies in a cyberattack that was traced back to Chinese servers. The attack appeared to have been an attempt to access the email accounts of Chinese human rights activists, and to target the source code of Google and various other US companies. A close reading of these articles reveals a much more sophisticated mobilization of the securitizing frame than that used in 1995 and 1996. The dominant framework in the Google-China incident is not purely one of securitization but also one of public-private partnership; these articles usually employ the two frames together. Google appears to be almost the test case for public-private collaboration over cybersecurity. This illustrates the influence that industry has on the international stage by necessitating that the U.S. government step in on behalf of Google in its conflict with

China. At the same time, the civil liberties frame is used to emphasize that 'do no evil' Google and the 'land of the free' are collaborating against an act of Chinese aggression against the U.S., and the repression of Chinese citizens. The definition of 'security' is beginning to shift, focusing on the defense of 'freedom'. After examining the original data set which includes all four keywords, it is revealed that initial reporting on the incident used the term 'cyberattack' rather than the more general 'cybersecurity', perhaps indicating a framing of the incident as a one-off rather than part of an ongoing security issue. In addition, the framing suggests that the attacks should be viewed as a company issue with broader implications for human rights, but that the industry itself and not the government should decide on a moral and economically viable response. The cybersecurity keyword and the 'security' frame appears more later on when the foreign policy implications start to be considered and Google's position as a representative of US business interests and potentially as a US national security asset starts to be talked about.

This analysis suggests that the framing of this incident is far more complex than could be ascertained from this data set. As a result, it was concluded that the Google-China incident should be analyzed as a separate case study using a new data set, gathered from the previously chosen news sources. This analysis has confirmed that the awareness of the national security implications of cybersecurity issues has grown over time, and that the way in which these concerns are framed is influenced by external socio-political facilitating conditions. It is also clear that the framing used in conjunction with the security frame suggests that private interests are being subsumed into national security concerns, as the importance of industry is acknowledged. Similarly, alternative tactics are being developed to handle civil liberties critiques, and the Google-China case seems to be a watershed moment in achieving this. Therefore the Google-China cyberattacks will be examined as a case study in order to examine the way in which different frames are mobilized to deal with a specific event, and how this framing continues to have an effect in future reporting.

Chapter 6.

Google vs. China: A Case Study

> There's little doubt this is a watershed moment for Google. By publicly contemplating a withdrawal from China, the company is showing it values its reputation for providing a secure service to users more than a leading position in a huge and growing market. (Peaple, 2010, para. 1)

The Cyberattack

The U.S. defines itself as the defender of the free world and as we have seen has emphasized both the threat of cyberattacks and the need to have free and open access to information. Google, as one of the more internationally successful representatives of the U.S. technology industry, had cast some doubt on this label due to its acquiescence to China's censorship requirements. This agreement was not beneficial to Google either as it contradicted its own identity as represented by its moto 'don't be evil'. However China was a large and lucrative market that any technology company would be hard-pressed to walk away from over ideological differences, and Google was unable to challenge the policies of the Chinese government without U.S. government backing. The U.S. government was unwilling to put pressure on the Chinese government due to its reliance on Chinese trade, a relationship that had faced significant troubles over the years on economic, national security, and civil rights fronts. China had previously been equally dependent on the U.S., but in recent years China has gained more economic independence and begun to assert its power (Bremmer, 2010). Due to the their unstable but essential relationship, the U.S. has been cautious about how it responds. Therefore the cyberattacks on Google gave the U.S. the perfect excuse to challenge China on censorship as Google's announcement was conveniently timed to coincide with Secretary of State Hillary Clinton's address on Internet freedom.

The Google cyberattack is significant for the securitization of cyberspace for a number of reasons. Firstly, it is a high-profile example of the kind of cyberattack that cybersecurity rhetoric has warned of, thereby justifying the implementation of certain extraordinary measures. Secondly, the framing of the Google cyberattack in the media reflects some of the key issues raised in the analysis of the cybersecuritization frame; namely the need for the collaboration of private industry with the government, the development of a cyber-industrial complex, and the justification for increased control and monitoring of cyberspace. Finally the most important effect of the framing of this incident for our purposes is that it changes the terms of the cybersecurity debate; rather than presenting civil liberties as a necessary casualty of increased security, the Google incident makes Internet freedom the target of the attacks, with Google and U.S. ideology as the representatives of this freedom. This is not the first time that this rhetorical strategy has been used; it has its history in the framing of the 9/11 attacks. As Vultee explains,"[w]hen President Bush told the nation that 'freedom itself was attacked this morning,' he was naming 'freedom' as a victim (Anker, 2005), but more importantly he was placing freedom at the core of the nation's identity" (2011, p. 81). Therefore a security response—even one that reduces privacy to a degree—is justified because it allows for the protection of a broader freedom. Rather than giving up a little of our individual civil liberties to guarantee our security, this trade-off is framed as an exchange for a more fundamental, global freedom.

The reporting on this incident focuses on three major concerns that are central to national security: physical safety, economic security, and civil liberties. Physical safety is threatened as China and the U.S. have historically been at ideological odds and were once on the opposing sides during the Cold War. The openness of the Internet is important as it provides a way for the U.S. to challenge Chinese ideology by opening up a channel whereby Western ideals can reach the Chinese people. China is also a major trading partner of the U.S. and is a nation upon which the U.S. largely depends for its economic security, while its attacks targeted the intellectual property of the U.S. technology industry. The economic discussion in the articles emphasizes the importance of China to American economic interests, and how Chinese policies threaten these interests. Finally China is known for its human rights infringements and closed-off ideology in contrast with the self appointed position that the U.S. holds as defender of the free world. The discussion of human rights in the reporting emphasizes that Google is in the right, encourages the U.S. to support Google, and highlights the role of the U.S. as defender of the free Internet and of Chinese dissidents. Therefore the framing of this incident converges around one or a combination of these three threat focuses.

The analysis of the framing of the Google-China incident will be broken into three parts. The first part will analyze the significance of the incident in terms of quantity and longevity of reporting. It will look at the shifting focus on the incident over time to see when it is the 'topic' of news reporting and when it functions as a schema to evoke a framing of or way of understanding future events. To this end the dominant frames in the reporting of the incident will be analyzed, as well as the frames evoked in references to the attack throughout the year. The second part will take a more in-depth look at the initial framing of the incident in order to assess how the articles mobilize the securitization frame, and how this reporting is reflective of more general cybersecurity media coverage. The final part will look at the policy discussions that are facilitated by the coverage of this significant incident. These policy debates will be assessed to see whether they fit the extraordinary measures that are prompted by the cybersecuritization frame.

Overview of the Coverage

A search for articles reporting on this incident throughout the year shows a continuing interest in the conflict and its long-term ramifications. The graph in Figure 5 shows how the level of interest in the incident fluctuated throughout the year, with the highest periods of sustained reporting composing almost a month of coverage following the occurrence of the incident in mid-January, and then again for around two weeks in March. In addition there are spikes in reporting in June and November, as well as sporadically and to a lesser extent throughout the year. The significance attributed by the media to the incident can be seen in the sheer number of articles which report on the cyberattacks during that first month of coverage—262 in total between January 13th and February 11th. Similarly the renewed interest in March results in 113 articles between March 23rd and April 1st.

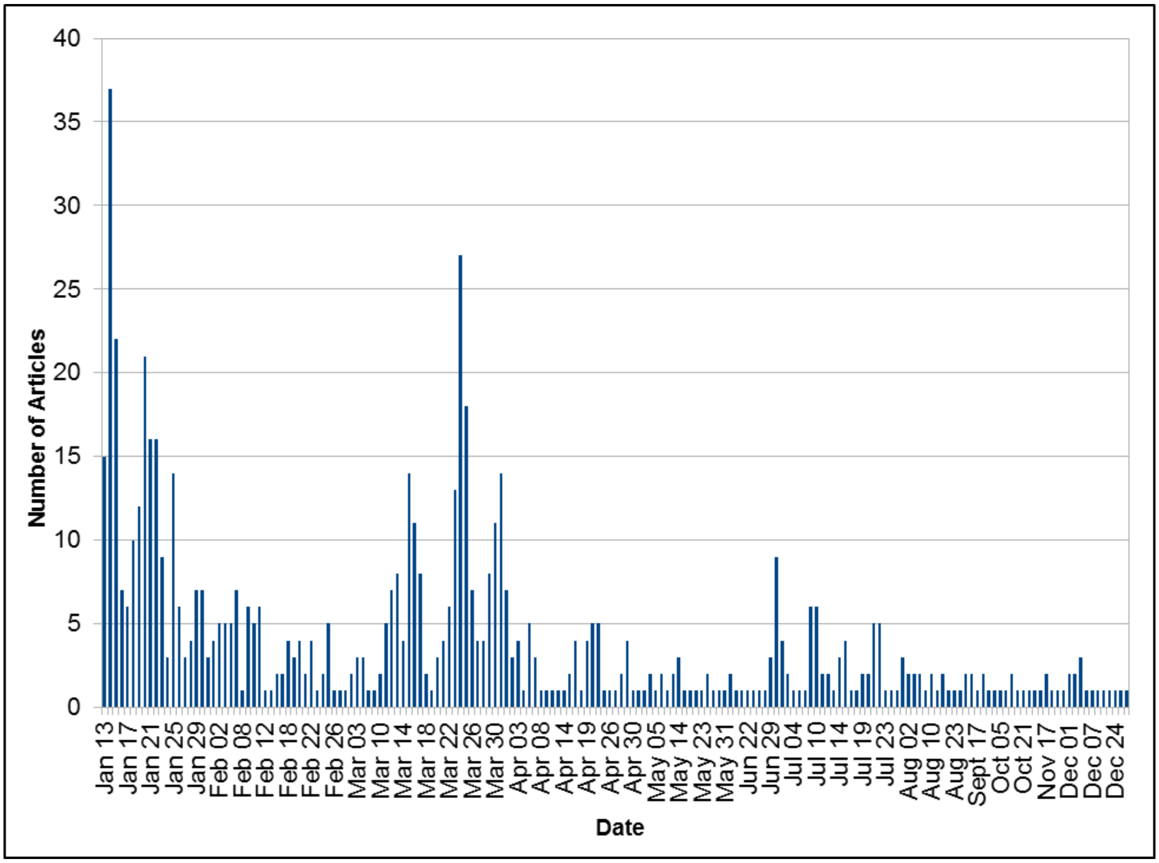

Figure 5. Number of Articles Reporting on the Google-China Incident by Date

A closer reading of the texts indicates that the initial sustained reporting occurs as details of the cyberattack are revealed, the relevant actors respond to the event, and the potential ramifications are discussed. The renewed interest in March is prompted by Google's long-deliberated decision to stop censoring its search results in China. The resulting furor of reporting indicates the continued interest in this conflict as it develops over time. This announcement was reported alongside developing problems between the U.S. and China over China's refusal to allow its currency to appreciate against the dollar, resulting in broader economic conflict and hardship. The Google cyberattack thus becomes an example of the negative impact that Chinese economic policies are having on American industry, as well as symbolizing a flashpoint in broader U.S.-Chinese conflict. The spike in June occurs as coverage responds to the latest flare up in tensions between Google and China, again indicating continued interest in the case, and its assumed importance. Google's license to operate in China is up for renewal, but there is some doubt as to whether China will renew it given their recent tensions. This results in news coverage expressing concern for Chinese citizens, as they may lose this essential portal to democratic, Western information should Google lose its battle against Chinese censorship. The final spike in November occurs not directly in response to further developments of Google-Chinese relations, but as a result of the Wikileaks 'Cablegate' incident, when confidential U.S. diplomatic cables were released publicly online. Through these cables, it is revealed finally that the Chinese government was behind the cyberattacks on Google, confirming largely unquestioned media and government speculation, and cementing the framing of the cyberattacks as a national security incident.

An analysis of the initial reporting on the Google cyberattack shows us how the incident was framed; however the fact that it continues to be referenced throughout 2010 indicates a continued interest in the attack and its significance. Therefore it is important to look at the framing used in these media sources throughout the year to see why the incident receives continued attention, and whether it begins to function as a schema or referent within articles of a different topic. Having conducted a close reading of the initial reports on the cyberattacks it is clear that the dominant frames in these accounts are those of national security, economic security, and human rights. Figure 6 illustrates the presence of these frames in articles reporting on the attacks throughout the year. There is a consistent, low level national security framing in articles which reference the incident, and higher frequencies of economic and human rights framing. We can see that a combination of these frames is often used. These combinations evoke human rights most frequently, with 184 articles using this frame; a close second in commonality is economic framing, which appears in 171 articles; the national security frame is used significantly less often, in 121 articles. This comparatively smaller frequency does not reduce the significance of the national security frame. As we have established, framing relies upon the reference of schemata, or the elements that are covered when outlining a specific activity—for example in security there is that which is threatened, an aggressor, and solutions. The national security frame is employed most frequently during the first month of media coverage. Therefore the framing in the initial coverage of the cyberattack as a national security threat means that references to Google and China in the future would call up this existing schema, in which Google as a representative of U.S.

democratic ideology and industry was threatened by China, necessitating Google's warning that it may discontinue its service, a démarche from the U.S. government, and an investigation by the National Security Agency. In such an event, overt national security framing would be unnecessary, as this would be implicit in the referencing of the incident itself.

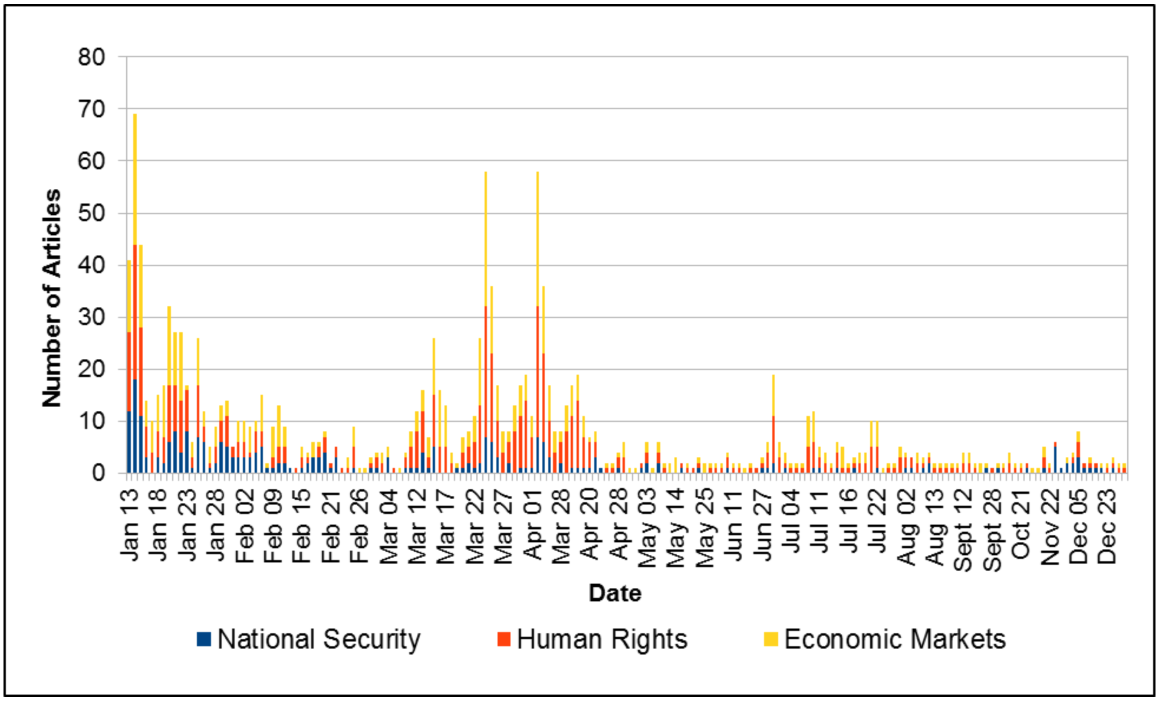

Figure 6. Frequency of Frame Usage by Date

Reporting of the initial incident

On January 12, 2010, Google posted an entry on its blog entitled “A new approach to China” which announced the company's discovery of a sophisticated cyberattack on its digital infrastructure that appeared to target its intellectual property and the email accounts of human rights activists. The origin of the attack had been traced to servers in China. The post emphasized the scope of the attack, stating that “at least twenty other large companies from a wide range of businesses--including the

Internet, finance, technology, media and chemical sectors--have been similarly targeted" (Google, 2010, para 2) prompting Google to take the unusual step of publicizing the incident and working with U.S. authorities to investigate the attack. Their decision to go public was reportedly, "not just because of the security and human rights implications of what we have unearthed, but also because this information goes to the heart of a much bigger global debate about freedom of speech" (ibid, para 6). By tying the cyberattacks the the broader issue of Internet freedom, Google was able to justify the need for a new approach in China that had in actuality been prompted by years of tension and conflict between the search giant and the Chinese government over censorship. Google's announcement coincided with (but was not ostensibly coordinated with) a speech that Secretary of State Hillary Clinton was due to give on Internet freedom. The story was widely reported in the mainstream media the following day, and received heavy coverage over the following week. During this time the Chinese government responded, Google attempted to come to a decision about its future in China, the attacks were investigated in an unusual partnership of private industry and U.S. intelligence, and the U.S. government initiated a delicate political dance to chastise but not alienate the Chinese government. In the following sections, the framing of the media coverage will be examined to see whether it is consistent with the way the cyberattacks were framed by Google and the U.S. government: as an example of Chinese aggression threatening Internet freedom. This analysis will also assess whether this assertion is indicative of the presence of a securitizing frame.

Direct National security threats

In several of the initial reports, it is alleged that a direct national security threat is posed by the cyberattacks. This threat is framed in one of two ways, the first of which is cyber espionage. It is asserted that it was not only U.S. industry that was targeted in the attacks, but also U.S. defence and strategic assets; for example *The Washington Post* suggests that the attackers "appeared to be after information on weapons systems from defense firms" (Nakashima et. al, 2010, para 6). Several other reports give credence to this suggestion by drawing parallels between the current attacks and past incidents involving China, for example several reports compare the attacks to a previously discovered electronic spying operation known as 'Ghostnet' which targeted government systems around the world (Jacobs and Helft, 2010, para. 23). It is stated that Chinese-based hackers routinely target Chinese dissidents and major U.S. assets such as the State Department, NASA and the World Bank as part of a "cyber-espionage campaign starting in 2003 [that] involved hackers systematically infiltrating thousands of computer systems in hundreds of countries" (Wall Street Journal, 2010, para 5). It is suggested that, "[w]hile there's no smoking gun, the Chinese military has heavily invested in equipping its cyber units, and there is a consensus in the U.S. defense community that the Chinese government at the very least tacitly supports thousands of hackers" (ibid). This assertion helps to frame the incident as likely a government-sponsored attack.

The second framing suggests that these cyberattacks are indicative of a more direct and troubling national security threat, and hints at the possibility for cyberwar. The connection is made between the cyberattacks and more traditional nation-state conflicts, for example "China's territorial claims or even the collision of an American spy plane and Chinese fighter pilot nine years ago" (Sanger and Markoff, 2010, para 11). The suggestion is made that these types of threats are outdated, and that the future battleground will be in cyberspace. One article asserts that the conflict is already in motion, noting that the Google cyberattacks illustrate "the degree to which China and the United States are engaged in daily cyberbattles, a covert war of offense and defense on which America is already spending billions of dollars a year" (ibid, para 12). *The Washington Post* reminds readers that "China is among a handful of countries considered to have impressive cyber-offensive capabilities" (Nakashima et. al, para. 25) and then lists as evidence a series of attacks since the 1990s in which China "or its broad army of proxies" was the "suspected aggressor." This list includes "Titan Rain, a campaign of cyberattacks against the Pentagon, nuclear weapons labs, NASA and defense contractors from 2003 to 2005; penetrations of the Commerce and State department networks in 2006; and GhostNet, a widespread spying operation targeting supporters of Tibetan independence in 2008" (ibid, para. 27). This is a distinctly more militaristic framing that highlights a long history of attacks by the Chinese state on U.S. strategic assets.

The *Wall Street Journal* takes this framing to its logical conclusion, publishing an article with the title, "Web Is New Front Among Cold War Foes; Attacks Against Multinational Corporations Would Represent a Significant Expansion of Targets Beyond the Military" (Gorman, 2010a). This is a clear securitizing move in which a previously established national security threat is invoked, raising the level of concern about the current threat. The article also suggests that an attack which targets corporations must be seen as an attack on U.S. industry and therefore a threat to the nation, stating, "[t]he Googles of the world are as important to U.S. national power and U.S. national security as some of the traditional elements of military power" (ibid, para 11). In support of this idea, many of the articles seem to refer to Google in place of or as the representative of the U.S. by using national security language to describe its relationship with China, for example 'clash', 'conflict' 'blew up' or 'uneasy truce'. The U.S. government's response to the attack is publicly guarded and diplomatic, however the *Wall Street Journal* points out that, "[t]he attack has piqued the interest of U.S. intelligence agencies, including the National Security Agency" (Vascellaro et. al, 2010, para 3), indicating that the incident was understood by security professionals to be a national security concern.

Therefore the initial reporting bears some of the hallmarks of securitization; the referent object is either Google as the ideological representative of the U.S., or U.S. industry and therefore the U.S. itself. The aggressor is unquestionably China, despite the lack of concrete evidence supporting this assertion. The threat is posed to U.S. ideology and economy, which according to the Copenhagen School would make this an existential threat as ideology and economy are fundamental to a nation (Buzan et. al, 1998). There are several security professionals or securitizing actors who are referenced repeatedly in these articles as emphasizing the importance of this threat, perhaps the most significant being President Obama. The *New York Times* points to Obama's repeated warnings about "the country's vulnerability to devastating cyberattacks" and calls the Google attacks one of the biggest examples of such an attack since he took office (Sanger and Markoff, 2010, para 5). Other major security professionals who are quoted directly in response to the attacks include Hillary Clinton (Secretary of State) David Drummond (Google's Senior Vice President and Chief Legal Officer), William J. Lynn (Deputy Defense Secretary), the Secretary of Commerce, members of the National Security Agency (NSA) and Department of Homeland Security (DHS), and various anonymous 'senior military officials'.

Google 'Don't be evil'

Google's international influence is highlighted throughout the articles, emphasizing the role that large corporations have in the international arena, although importantly it is portrayed as an American company, not an independent actor. The majority of the articles depict Google as an organization that believes that information should be free. More than that, some reports frame Google in highly altruistic terms, citing its moto 'Don't be evil' as guiding its actions. One article from *The Washington Post* praises Google for having “taken a bold and difficult step for Internet freedom in support of fundamental human rights” (Nakashima et. al, 2010, para. 16), while another from *USA Today* asserts that Google is “championing human rights” (Acohido and Swartz, 2010, para. 3). Its past decision to abide by Chinese censorship laws is described as one of the “painful concessions” the company has had to make in order to gain access to this huge market (Dean, 2010, para. 1), however it is claimed that human rights trump Google's desire for financial success, as representatives are quoted as saying “[w]e are not going to make a financially based decision to stay in a market that is intolerable for us” (Helft, 2010, para. 7). Interestingly, none of the articles emphasize the fact that freedom of information is essential to Google's business plan. Rather the motivations for these decisions are said to be based on the personal desires of one of the company's founders Sergey Brin, who, the articles emphasize, spent his childhood in the oppressive Soviet Union (Cohen, 2010). Google is therefore 'in the right' both in its moral stance and in the sense that it was the innocent victim of Chinese aggression. The framing of Google as inherently 'good' is significant because in this narrative Google represents the United States, both in its ideology, and as one of the most successful companies in technological innovation, an achievement which is made possible by the openness and free market mentality characteristic of the U.S. In addition, references to censorship and control under the Soviets along with more direct references to the Cold War situate Google as a major player in a much broader clash of ideologies, similar to major national security threats of the past.

Censorship

While Google's decision to leave China was prompted by an attack on its digital infrastructure, its public statement along with comments from the U.S. government ensure that these attacks are firmly tied to the issue of censorship. A degree of confusion is evidenced by the news sources over what should be the central focus of the reporting; they emphasize the cyberattacks as the main issue, or focus on censorship with the attacks mentioned almost as an afterthought. An article in *USA Today* points out the stretch in logic that the public is asked to take, stating, “[t]hough cyberattacks and government censorship are separate matters, Google blended them in one sentence” referring to Google's statement that “[t]hese attacks and the surveillance they have uncovered --combined with attempts over the past year to limit free speech on the Web --have led us to conclude that we should review the feasibility of our business operations in China” (Acohido and Swartz, 2010, para. 6). This statement could be read as indicating that Google has decided to use the attacks as an opportunity to finally 'do the right thing', or it could be seen as an indication that the company was happy to go along with Chinese oppression so long as it was being treated well by the government, and that the attacks were an insult that required a strong response. The articles for the most part emphasize the former interpretation. The *Washington Post* highlights the longstanding ideological conflict over Google's desire “to provide quick, unfettered access to information, and over the Chinese government, which wants to restrict its citizens' access to politically sensitive topics and to monitor their activity” (Nakashima et. al, 2010, para.11), while the *New York Times* blames China's attempts to “limit free speech on the Web” (Jacobs and Helft, 2010, para. 1). Google's previous acquiescence to censorship is justified by the argument that the company had previously thought that even its censored services would be better than nothing at all, however the *Wall Street Journal* notes that “a Google withdrawal would also be an implicit rejection of the argument made by many technology companies that their presence in China overall helps expand access to information for Chinese citizens, despite censorship” (Vascellaro et. al, 2010, para. 24). In this sense Google's decision is seen to have even broader impact, as it draws the ideological battle lines between U.S. companies and Chinese governance. Even broader potential implications are hinted at as a Beijing telecom representative is quoted as stating, “[n]o issue with an American company has a greater potential to impact popular perceptions of China in the U.S. and the views in Congress” (Dean, 2010, para. 2).

US ideology

The framing of the ideological conflict between Google and China highlights the broader ideological conflict between the U.S. and China; in fact the *Wall Street Journal* asserts that Google is “defending a brand steeped in American values” (Areddy, 2010, para. 9). While the U.S. is reticent to respond directly to the Chinese attacks due to the complex and interdependent relationship between the nations, the framing in these articles emphasizes that the nations are at odds on the issue of censorship, and that Google's response could be read as the indirect response of the U.S. government (Solomon et. al, 2010, para. 1). The close relationship between Google and the U.S. government is emphasized throughout the articles, which state that while the two did not coordinate on Google's response, Google executives did notify U.S. officials of their intentions beforehand. A *Washington Post* article quotes a cybersecurity expert as stating "[y]ou couldn't have picked a worse company to hack if you wanted to not irritate the Americans... They're their favorite child" (Nakashima, 2010b, para. 8). At the time of Google's announcement, the media is also highly aware of an upcoming policy speech by Secretary of State Hillary Clinton on Internet freedom. While the speech does not occur until a week after the first reports of the Google attacks, it is repeatedly mentioned in the articles. They also highlight President Obama's very public stance on Internet freedom; a Wall Street Journal article reminds readers of Obama's “speech on the importance of open Internet use during a trip to China in November” at which “the president described himself as a "big supporter of noncensorship” (Back and Vascellaro, 2010, para. 3). Through this framing, the reader can infer the position of the U.S. government towards the cyberattacks.

US responsibility to liberate Chinese Citizens

Calls to combat Chinese censorship are addressed interchangeably to Google and the United States throughout the articles, illustrating how the framing of this ideological conflict indicates that this is an incident with national security implications despite the U.S. government's reluctance to make a strong response. The *Washington Post* quotes a Chinese dissident as saying that “Google should “not abandon” China but rather apply pressure through the World Trade Organization and U.S. government” (Nakashima et. al, 2010, para. 21), emphasizing the responsibility that both Google and the U.S. has to defend the rights of the 'oppressed' Chinese people. The article also highlights ongoing efforts by the U.S. to promote freedom of information in China, explaining that “[t]he State Department has set aside funds to help companies get around Internet firewalls put up by China and other countries” (ibid, para. 30). In support of the argument that Google believed its presence in China “would provide more information and openness to Chinese citizens” (Jacobs and Helft, 2010, para. 14), an article in the *New York Times* explains that “many Chinese dissidents used Gmail because its servers are hosted overseas and that it offered extra encryption” (ibid, para. 17). These arguments support the idea that the presence of U.S. technology companies in China is essential in order for the Chinese people to enjoy the kinds of personal freedoms to which readers in the West are accustomed. This existing and called-upon intervention by the U.S. has undertones of a call for liberation, and there are suggestions that more should be done. It supports the framing of the U.S. as the saviour of the Internet and the bringer of freedom and democracy, while the Chinese government is portrayed as repressive and controlling. Chinese censorship policy is described as “cyberoppression” (Kristof, 2010, para. 2) while the U.S. is “a leading source of 'hacktivists' who use digital tools to fight oppressive regimes” (Goldsmith, 2010, para. 5).

Foreign Policy

Despite the U.S. government's reluctance to publicly condemn China's actions, the media's coverage frames the incident as one which will have foreign policy ramifications. Questions posed to government representatives attempt to draw out a response on the broader implications of this situation. The White House responded with non-committal statements such as, “the president has strong beliefs about the universal rights of men and women throughout the globe. Those aren't carved out for certain countries” (Back and Vascellaro, 2010, para. 6). However the articles repeatedly emphasize the idea that the conflict between Google and China could become a national security incident; the *Washington Post* calls Google's response “a threat that could rattle U.S.-China relations” (Nakashima et. al, 2010, para 1), while a *Wall Street Journal* article carried the headline, “White House, Beijing Joust Over Censorship” (Back and Vascellaro, 2010). Several articles also place the incident in the context of wider U.S.-

China conflicts, further emphasizing the national security frame. The *Wall Street Journal* asserts that

> Google's move threatened to add to a growing list of disputes between the U.S. and China. Tensions have run high over the nation's trade imbalance and China's currency, as well as the push for a global climate-change agreement. This week, China tested a missile-defense system in a move widely viewed by Washington as a response to an expected U.S. weapons sale to Taiwan. (Solomon et. al, 2010, para. 3 and 5)

In another article, the *Wall Street Journal* points out that cybersecurity has also been a longstanding source of conflict between the two nations, and that at the same time as the Google cyberattack occurred, “representatives from a think tank associated with China's intelligence service met with U.S. specialists in an effort to reduce tensions over allegations of Chinese cyber spying” (Vascellaro and Solomon, 2010, para. 14 and 15). In another article the *Wall Street Journal* emphasizes the role of China as the aggressor, both in these attacks and in its more general dealings with the U.S., stating that “[a]ll of these tensions are taking place at a time during which China is rethinking what constitutes its national interests and how to secure them” (Solomon et. al, 2010, para. 7 and 5). This context elevates the threat level of the incident, framing it as the latest in a series of clashes between two great world powers.

American Economic impact

However as much as Google would like to have the public believe that its decision to leave China was a moral one, this incident and the broader clash of ideologies between the U.S. and China are as much issues of economy as they are of freedom. Many articles do express scepticism of the apparent altruism behind Google's decision and point instead towards its failure to succeed in the Chinese market as its real reason for pulling out of China, however this in itself does not negate the overall ideological argument. In fact it reinforces arguments that China's actions threaten American industry and therefore the U.S. economy by highlighting the fact that China promotes an unfavourable climate for foreign business. The articles emphasize the sheer number of companies who were victims in these attacks; that it was not just Google but potentially as many as 34 organizations that were targeted (Nakashima et.

al, 2010, para. 4), while others suggest that many of the victims were companies from Silicon Valley (Jacobs and Helft, 2010, para. 5), highlighting a particularly American industry that was targeted. The *Washington Post* states that the attackers “were seeking companies' “source code,” the most valuable form of intellectual property because it underlies the firms' computer applications” (Nakashima et. al, 2010, para. 6) and emphasizes that “this attack was so pervasive and so essential to the core of Google's intellectual property that only in such a situation would they contemplate pulling the plug on their entire business model in China” (ibid, para. 3). The suggestion therefore is that China attacked American industry to steal corporate secrets essential to that industry, so as to advance its own technological progress. The *New York Times* notes that “China is arguably the world's most important market outside of the U.S. You don't walk away from that on principle” (Helft, 2010, para. 12), suggesting an unresolvable conflict that is fundamental to the company's operations. The articles emphasize that China has made staying untenable, speculating on the influence Google's decision may have on other U.S. companies, and suggesting that this may have broader economic repercussions. This discussion of the national economic impact allows for frames that would usually be used in criminal situations to be incorporated into wider national security concerns; for example intellectual property theft, hacking, and corporate espionage.

Several of the articles point out that the attacks occurred as China's economic independence has been growing, and its protectionist policies have been causing tensions with foreign businesses and national governments alike. The *New York Times* asserts that “[a]s nationalism and protectionism builds in China... many technology companies have scaled back their ambitions there, particularly regarding content” (Helft, 2010, para. 4) suggesting that China's economic policy has caused problems for American industry abroad. As the reporting on the incident continues, this national economic frame is repeated more frequently, and it is suggested that China's protectionist policies are exacerbating the growing international economic crisis. China's refusal to allow its currency—the yuan—to appreciate against the dollar is highlighted, setting the Google cyberattacks in a wider context of Chinese actions that threaten the economic safety of the U.S. Similarly, the articles question China's respect for the rule of law, given the fact that the government refuses to enforce intellectual property law and that the U.S. suffers as a result of the sale of pirated material (Bolton, 2010, para. 2).

The *New York Times* explains that "[a]lthough China has agreed to World Trade Organization rules barring the theft of [intellectual] property, Internet companies here routinely stream American and other movies free over their Web sites, without apparent consequences (Wines, 2010, para. 21). This lack of enforcement highlights the need for private-public collaboration between industry and the U.S. government, in order to be able to put pressure on the Chinese government to enforce these laws. The Google cyberattacks are a clear test case for this collaboration, as intellectual property was assumed to be one of the targets of the attacks. It is proposed that "[t]he U.S. government and American businesses should do what they naturally do elsewhere: defend their own interests vigorously" (Bolton, 2010, para. 8), clearly suggesting the assumption that the Google incident will have broader foreign policy effects.

How to respond?

Despite some initial acknowledgement that the Chinese government denied its involvement in the cyberattacks and that no definitive proof existed to indicate otherwise, China quickly became the source of the threat subject in the securitization frame. Some articles clearly highlight the lack of consensus over the identity of the attackers, stating that "[t]he Chinese government has disputed that it was the source of the attacks" (Hernandez, 2010, para. 11) and that investigators have "stopped short of directly accusing the Chinese government of masterminding the attacks" (Helft and Markoff, 2010, para. 15). However other articles reference sources who accuse the Chinese government directly; for example the *New York Times* suggests that Google has "evidence leading them to the conclusion that the Chinese government was behind the attacks" (Markoff, 2010a, para. 2), and another article quotes a cybersecurity expert as stating that "[e]verything we are learning is that in this case the Chinese government got caught with its hand in the cookie jar" (Sanger and Markoff, 2010, para. 16). Despite the inability to definitely prove that the attacks were authorized by the Chinese government, the framing of the articles leads the reader to this conclusion. References to the Cold War and to pre-existing or long-term conflicts with China evoke schema in which China is understood to be an enemy of the U.S., or at least an antagonist or competitor. For example the *New York Times* notes that

> [o]ver the years, there have been private warnings issued to China, notably after an attack on the computer systems used by the office of the defense secretary two years ago. A senior military official said in December that that attack "raised a lot of alarm bells," but the attacker could not be pinpointed. (ibid, para. 17)

This indicates that difficulties have been encountered regarding attribution in the past, when the Chinese government was similarly implicated. Another article suggests that these attacks are carried out by “so-called patriotic hackers in China” who some U.S. security professionals see as “simply irregular elements of the People's Liberation Army” (Helft and Markoff, para. 15). Similarly the attacks are talked about in the context of long-term conflicts between Google and the Chinese government. Google contributed to this framing by releasing a statement in which it attributed its decision to pull out of China to both the attacks and “attempts over the past year to limit free speech on the Web” (Google, 2010). This framing is then taken up by news sources which state that Google had been the victim of a cyberattack, and was questioning its position in China following years of conflict with the Chinese government. The Chinese government is the clear aggressor in the conflicts with Google over censorship, so by mobilizing this existing schema through the direct linking of censorship and the cyberattacks, the Chinese government is made to stand in as the aggressor in the cyberattacks as well, despite the murkiness around the possibility of their being state-sponsored or independent attacks.

This use of China within the securitization frame presents problems for the U.S. government, as it demands a reaction, but the type of response called for is uncertain. As we have seen in previous chapters, there is little consensus over how to respond to a cyberattack, and this is even further complicated when the attacks cannot be concretely attributed. In addition, the complex relationship between the U.S. and China means that this uncertainty could lead to a volatile situation if erroneous accusations were made, or heavy handed responses used. As a result the Obama administration responds cautiously and this is reflected in the articles; several note that the administration has sent messages to the Chinese to “voice its concerns” over the attacks (Landler and Wong, 2010, para. 13), while another states that the administration would “look to Chinese authorities to conduct a thorough investigation of the cyber intrusions” (Kang, 2010, para. 2), perhaps issuing an “official protest” (Nakashima, 2010b, para. 1). The language is very passive; there are no demands made and no rebukes, as compared to the framing of Google's response to China. This passive stance reflects the difficult situation in which the U.S. government finds itself, and which the *New York Times* acknowledges, stating,

> [t]here is, in fact, an intense debate inside and outside the government about what the United States can credibly threaten. One alternative could be a diplomatic demarche, or formal protest, like the one the State Department said was forthcoming, but has still not delivered, in the Google case. Economic retaliation and criminal prosecution are also possibilities. (Markoff et. al, 2010, para. 8-9)

Obama's Inaction

President Obama is repeatedly characterized as promoting Internet freedom and is quoted as having described Internet access as a fundamental human right, aligning the administration and the U.S. with freedom and democracy, while by contrast China favours control, censorship, and oppression. However the inaction of the Obama administration in response to this attack on U.S. industry specifically and freedom more generally is also repeatedly emphasized; besides the demarche to China no direct action has been taken. The Obama administration is described as “frozen” as it cannot publicly condemn China without evidence (Sanger et. al, 2010, para. 4). Even though there is “little doubt” that the attacks were directed by the Chinese government, an accusation without proof would have serious ramifications on the already precarious and essential relationship of the U.S. and China (ibid, para. 15). The securitizing frame emphasizes the urgency of the situation and ties the incident to well-established cybersecurity rhetoric, reminding readers that Obama has “repeatedly warned of the country's vulnerability to devastating cyberattacks” (ibid, para. 5) and calling the incident “one of the biggest cyberattacks of its kind” (ibid, para. 15). This framing highlights the need for action to be taken, however the uncertainty around the source of the attacks makes this difficult.

The timing of Google's announcement is a key influence on the framing of the cyberattacks. The media was aware that Hillary Clinton was due to give a speech on Internet freedom the following week and it is therefore referenced with anticipation throughout the reporting of the Google attacks. The clear stance that the Obama administration had taken on Internet freedom and the approaching very public speech helps to immediately situate the U.S. in a morally righteous position. By the time the speech occurred on January 21, the media sources sampled here had already published well over one hundred articles referencing the cyberattacks. The importance of this speech as a statement of U.S. policy on Internet governance is clear, with the *Wall Street Journal* referring to it as “The Clinton Internet Doctrine” (Wall Street Journal, 2010b). Interestingly this is not a presidential doctrine, it is attributed to the Secretary of State and to Clinton specifically rather than to President Obama or his administration. References to President Obama throughout the articles are largely critical, highlighting his inaction and his largely verbal support of Internet freedom, whereas Clinton's speech is framed as an indication of the direction in which *she* is taking policy. One *Wall Street Journal* article gives “kudos” to Clinton and calls on the public to “support Mrs. Clinton for taking America on the offensive in the fight for electronic freedom” (ibid, para. 5). By contrast, a *Washington Post* article from the 'cybersecurity' data sample highlights the “Review Revue” that had become “a hallmark of [Obama's] governing style” (Milbank, 2010, para. 6) and questioned whether this cool deliberation was a welcome change after “eight years of seat-of-the-pants leadership”, or whether the President was too “slow and wavering” (ibid, para. 6). The differentiation between Obama and Clinton's policy approaches that is made by the news sources is exemplified in a *Wall Street Journal* article which states that this news source has often been disappointed with the lack of direct action President Obama has taken to support democracy activists, however “if Mrs. Clinton makes good on her promise, and if unrestricted Web access becomes a priority in Washington, she will have taken her Administration in a notably better direction” (Wall Street Journal, 2010b, para. 6).

The Clinton Doctrine

Presidential doctrines are usually clear foreign policy statements and this is no exception, with the language of the speech that is quoted throughout the articles illustrating the move to classify the Internet as a national security concern. Using a Cold War metaphor, Clinton points to several nations (namely China, Tunisia, Uzbekistan, Vietnam and Egypt) as places where “a new information curtain is descending” (Wall Street Journal, 2010b, para. 4). This metaphor is taken up and repeated throughout the articles; for example a *New York Times* article compares the Clinton Doctrine's support for organizations that allow for the circumvention of online censorship, to “anticommunist programs during the cold war, when the United States government backed broadcasters like Radio Free Europe” (Stone, 2010, para. 5). The same article also asserts that this policy has resulted in “a never-ending technological arms race” as the censors improve their methods, while pro-democracy organizations are constrained by a lack of resources (ibid, para. 7). The framing here and the comparison to Cold War scenarios also highlights a moral imperative similar to that of previous major ideological conflicts. The suggestion is that the U.S. has a responsibility to intervene in China's anti-democratic practices on behalf of the Chinese people, much as it did with the Soviets during the Cold War. The sentiment expressed in the Clinton Doctrine mirrors the framing in the news reports of Google's responsibility to provide an uncensored service to the Chinese people, and to “not abandon” China (Nakashima et al., 2010, para. 21). While Clinton does not directly accuse China of being behind the cyberattacks on Google, the media sources make this connection for her. The *Wall Street Journal* quotes Clinton as stating that, “[c]ountries or individuals that engage in cyberattacks should face consequences and international condemnation... In an interconnected world, an attack on one nation's networks can be an attack on all”(Wall Street Journal, 2010b, para. 1). The comments are then contextualized by stating that they “[follow] attempts by Chinese hackers to read the emails of human-rights activists by attacking Google's servers” (ibid).

However this framing isn't entirely clear-cut; *USA Today* points out the difficulty Clinton may have in selling Internet freedom rather than government control when Google's success hinges on its ability to appropriate and organize information to its own benefit. Viewed without the moral frame, the news source asserts that “China and Google take for their own purposes all the information in the world they can get their hands on” (Fishman, 2010, para. 6), suggesting that the search giant is no different to the Chinese government. However the article poses this problem within a moral, civil liberties frame; it begins by accusing China of “stealing the gems of America's knowledge economy, and [using] state-run censorship as an economic tool that targets American companies and aids domestic firms the Chinese government favors” (ibid, para. 1). The article ends on a similar note with an analogy for China's behaviour, asking the reader to imagine

> that Americans were allowed to steal, without consequence, all the most valuable stuff China sends here. Imagine if the U.S. government orchestrated, or refused to clamp down on, the looting of every Chinese container ship that hit our shores filled with Chinese goods. That is essentially the treatment the world's knowledge economy gets in China. (ibid, para. 16)

The conclusion then is that while Google and China's manipulation of information might seem similar in some respects, the actions of the former result in free and open access to that information, while the latter facilitates criminal activity that damages the U.S. economy. The speculation in this article over the importance of the framing that Clinton will use in her speech illustrates the importance of official frames as indicators of policy. This idea is also supported by an article in the *New York Times* which reports China's desire to portray the conflict with Google as 'not political', voicing concern that “the tone of [Clinton's] comments could propel the Google dispute in a more ideological direction, spurring incendiary speech on one side about the quashing of media freedoms and on the other about Western neo-imperialism” (Wong et. al, 2010, para. 7). While the Chinese government might be keen to keep the discussion from reaching an ideological level it is clear from the reporting in this media sample that such framing is already well underway. Indeed the anticipation around Clinton's speech and its perceived indication of policy direction confirms that the issue is already very political.

The Google cyberattack is therefore important because it was a clear cybersecurity incident that was immediately followed with a clear statement on cybersecurity policy, marking it as significant to national security. The *Washington Post* notes this move, stating that the Obama administration “has raised concerns about cybersecurity and Internet freedom with China before. But by formally protesting to the Chinese, the United States is elevating the issues to a new level” (Nakashima, 2010b, para. 8). The *Wall Street Journal* also asserts that this policy shift is an indication of the “growing role of the Internet in foreign policy” (Gorman, 2010b, para. 2). The article also draws the link between the importance of the Internet to foreign policy and the understanding of “Internet freedom as critical to America's longstanding promotion of democracy abroad” (ibid, para. 5), and it notes that the U.S. had recently been negotiating with Russia and China on cybersecurity (ibid, para. 8). This article therefore situates the response to the Google cyberattacks within broader developments in cybersecurity policy.

Attribution: Cybersecurity's Extraordinary Measure

The discussion around the issue of an appropriate response to such an attack is characterized by the doubt surrounding both the origin of the attacks and the extent of the Chinese government's involvement, which leaves President Obama unable to respond in a way that would be adequate for the level of threat being portrayed. This highlights a central policy implication for cybersecuritization; the need for attribution. The *New York Times* notes that “[f]or years the National Security Agency and other arms of the United States government have struggled with the question of 'attribution' of an attack” (Sanger and Markoff, 2010, para. 8) illustrating the fact that this problem has long hamstrung those responsible for national security. The serious implications of this impediment are emphasized as the article draws the connection between this attack and warfare, noting that “what makes cyberwar so unlike conventional war is that it is often impossible, even in retrospect, to find where the attack began, or who was responsible” (ibid, para 8). The majority of the articles do not consider in any detail how such attribution could possibly be attained. There is also no consideration of the implications of the ability to attribute attacks, i.e. the removal of anonymity online, and the increased monitoring of computer networks.

However one article does draw this conclusion; a piece in the *Washington Post* authored by previous Director of National Intelligence and Director of the National Security Agency, Mike McConnell (2010). The decision to give McConnell a mouthpiece is significant in the light of the Copenhagen School's discussion of which actors are able to perform the securitizing act, and the news source's decision to publicize certain actors' views. Through this article it is made clear that, using the cybersecuritization frame, attribution is the solution whose implementation will require 'extraordinary measures' to be taken. In the clearest example of securitizing rhetoric in this data set, McConnell pronounces that, “[t]he United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking” (ibid, para. 1). Having established the U.S. as the referent object, and cyberwar as the threat subject, he then raises the level of urgency by using the spectres of the Cold War and the Global War on Terror as comparisons to the current threat. He calls for a cybersecurity strategy that draws lessons from both of these long-term conflicts by incorporating both deterrence and preemption. Attribution is key for both strategies: it is impossible to deter attacks or to preempt them when the enemy is unknown. Therefore, he argues, it is necessary to "reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment -- who did it, from where, why and what was the result -- more manageable" (ibid, para. 12). What McConnell proposes can only be called an extraordinary measure; a fundamental altering of the Internet from what some have called a "global commons" (Deibert, 2003; Deibert et. al, 2010; Saco, 1999), to a medium of communication that is closely monitored and tightly controlled. In addition, his ideas suggest the development of what Tate and Watkins have referred to as a 'cyber-industrial complex' (2011); McConnell calls for "robust investments" because "security never comes cheap" (2010, para. 21). He argues that, the Cold War required the U.S. to "[invest] heavily in our response capabilities with intercontinental ballistic missiles, submarines and long-range bombers, as well as command-and-control systems and specialized staffs to run them" and that "[t]he resources available were commensurate with the challenge at hand -- as must be the case in cyberspace" (ibid, para. 8).

The frames used in the initial coverage of the Google incident also feature prominently in this article, and McConnell uses the incident to support the need for his cybersecurity strategy. Firstly, McConnell directly references the Google attacks as evidence that the U.S. is currently embroiled in a cyberwar, stating "[t]hese battles are not hypothetical. Google's networks were hacked in an attack that began in December and that the company said emanated from China" (ibid, para. 4). The economic impact is framed similarly to the previous articles which suggest cyberattacks such as those against Google are an attack on U.S. industry and therefore the economy; McConnell asserts that "[t]o the extent that the sprawling U.S. economy inhabits a common physical space, it is in our communications networks. If an enemy disrupted our financial and accounting transactions, our equities and bond markets or our retail commerce... chaos would result" (ibid, para. 3). The methods of deterrence that McConnell suggests seem to be in line with the statements made in Clinton's speech; he compares the Cold War mantra that "a strike on one would be a strike on all and would be met with massive retaliation” to Clinton's statement that “[c]ountries or individuals that engage in cyber-attacks should face consequences and international condemnation... In an Internet-connected world, an attack on one nation's networks can be an attack on all” (ibid, para. 10-11).

The response he advocates to a cyberattack is very similar to the response Google chose, making this incident an ideal example; Google invited the NSA to investigate the intrusions into their systems, giving the intelligence agency access to their digital infrastructure and potentially their customers' data. McConnell justifies the involvement of the NSA in domestic affairs by arguing that it is “the only agency in the United States with the legal authority, oversight and budget dedicated to breaking the codes and understanding the capabilities and intentions of potential enemies” (ibid, para. 15). Further, he calls for public-private partnership and collaboration; a common frame in discussions of cybersecurity. He laments the restrictions placed on government and security professionals in terms of their ability to be involved in the affairs of industry, stating that “the private sector needs to be able to share network information -- on a controlled basis -- without inviting lawsuits from shareholders and others” (ibid, para. 16). Again Google provides an ideal example because its announcement of the cyberattacks marked a watershed moment; rather than keeping quiet and dealing with the breach internally as private industry usually does, it made a public announcement and invited government involvement in investigating the attacks. Google is thus a posterboy for the cybersecurity strategy McConnell envisions.

Policy Implications

By comparing the spikes in the Google-China data set with the 'cybersecurity' data set, it is possible to infer links between the cyberattack and the development of cybersecurity policy discussions. Looking at the articles in the 'cybersecurity' data set that were published immediately before the cyberattacks were announced gives us context for the way the cyberattacks were framed, and the message that securitizing actors might have wanted audiences to take away. Similarly looking at the policy discussions following the attack and the way in which they have shifted can indicate whether the securitizing actors' manipulation of the framing of the attacks had the desired effect.

An article from the 'cybersecurity' data set published before the cyberattack on Google's infrastructure reported on the stalled progress regarding the 'standing up' or activation of the U.S. Cyber Command, the organization which was to officially take charge of coordinating military cybersecurity efforts (Nakashima, 2010c). Concerns over privacy issues are cited as being the source of this delay, as it is unclear what kind of relationship the command will have to the National Security Agency, which legally is only supposed to be responsible for foreign threats, not those on domestic soil. The civil liberties frame is apparent in the reporting as the article questions the NSA's involvement, stating that “[t]he NSA has the skills and authority to encrypt military secrets and break enemy codes, but its involvement in the controversy over warrantless wiretapping several years ago has raised concerns about any role it will play in a cyber command” (ibid, para. 5). By drawing the readers' attention to the NSA's previous overstep of its bounds the article invokes the schema of government surveillance of U.S. citizens, creating a feeling of distrust. It also points out that the monitoring of private networks may be necessitated, raising concern that “purely private, non-government communications could be monitored” (ibid, para. 12). While the article does not question the need for the command, it does continually return to the question of privacy, noting “the past controversy” involving the NSA and the subsequent need for oversight (ibid, para. 18). The article is similarly concerned with the mission of the new command, over which there seems to be a lack of clarity around a clear national cybersecurity strategy (para 4). This is further complicated by a similar lack of clarity over how a cyberwar would be conducted; the article notes a “dizzying array of policy and doctrinal questions involving cyber warfare” that include

> [w]ho should authorize a cyber attack on an adversary that might be capable of undermining the United States' financial system or energy infrastructure? What degree of certainty is needed about an alleged attacker before authorizing a response? When does an effort to defend a U.S. military network cross the line into an offensive action? (ibid, para. 23-24)

The Google-China incident serves to clarify many of these questions, highlighting the importance of collaboration between the government and private industry, cementing the role of the NSA in investigating such an attack, and providing a clear example of what a cyberattack would actually look like. It also enhanced the immediacy of the threat, perhaps thereby undermining the argument in favor of careful deliberation to ensure the protection of civil liberties.

Following the cyberattacks, several articles note the NSA's involvement in investigating cybersecurity issues, and with the Google case in particular, but only three discuss the implications of this involvement. One is the McConnell article which, as we have seen, champions the NSA's involvement in cybersecurity development. The other two articles appear to place privacy front and centre, or so their titles suggest; the first article from the *Washington Post* claims that the deal between Google and the NSA “raises issue of privacy vs. security” (Nakashima, 2010d), while the second article from the *New York Times* emphasizes in its title that the NSA is a “spy agency” (Markoff, 2010b). However while privacy concerns are voiced, the dominant frame is that of private-public partnership; a development that is portrayed in a positive light. The *Post* article heavily utilizes terminology which emphasizes the collaborative nature of the endeavour, including “teaming up”, “agreement”, “help”, “partnership”, “alliance”, “share”, and “pact” (Nakashima, 2010d). Similarly, the *Times* uses terminology such as “work together”, “cooperative research and development agreement”, “relationship”, “partners”, “reaching out”, “collaboration”, and “assistance” (Markoff, 2020b).

Both articles do highlight the fact that this partnership carries civil liberties and privacy implications, but rather than placing security and privacy in opposition or suggesting a trade off, the *Post* refers to this relationship as a “balance” (Nakashima, 2010d, para. 4). Both articles acknowledge the significance of this issue, with the *Post* stating that it “strikes at the core of one of the most sensitive issues for the government and private industry in the evolving world of cybersecurity” (ibid), while the *Times* states that it “raises... civil liberties issues” (Markoff, 2010b, para. 2) and “reopens long-standing questions about the role of the agency” (ibid, para. 10) and yet neither article offers any answers to or opinion on these questions. A privacy expert is quoted by the *Post* as being “a little uncomfortable” about the agreement (Nakashima, 2010d, para. 17), while an expert quoted by the *Times* uses stronger terms, stating that “Google and

N.S.A. are entering into a secret agreement that could impact the privacy of millions of users of Google's products and services around the world” (Markoff, 2010b, para. 11). However this critique is mitigated by fact that it is immediately followed by securitizing testimony from the Director of National Intelligence, who states that “the threat of a crippling attack on telecommunications and other computer networks was growing, as an increasingly sophisticated group of enemies had ''severely threatened'' the sometimes fragile systems behind the country's information infrastructure” (ibid, para. 12). The potential privacy ramifications are played down as both articles note that it is not unusual for technology companies to draw on the NSA's expertise and ask for guidance in network defence (Nakashima, 2010d, para. 14, and Markoff, 2010b, para. 9).

Several articles published in the months following the cyberattack cover the exploration of public-private collaboration on a policy level following the example given by the Google-China incident. Two articles raise the possibility of public-private collaboration being enshrined in cybersecurity law as they discuss the Cybersecurity Act, legislation proposed by Senators Rockefeller and Snowe. The first article was published in late February and coincides with the period immediately following the cyberattack and with McConnell's proclamation that the U.S. is embroiled in a cyberwar that it is losing. The second article was published in mid-March and coincides with Google's announcement that it would stop censoring in China, prompting renewed focus on the issue and perhaps further cybersecurity policy debate. The first article primarily argues for the government's need to “become more aggressive in getting industry to protect computer networks because self-regulation is not working” (*The Washington Post*, 2010c, para. 1) mirroring earlier discussions about President Obama's indecision and the need for decisive action rather than reviews. A pro-regulation frame is therefore prominent in this article, in contrast with earlier tendencies towards anti-regulation framing. Experts are quoted as stating that “[t]he government needs to give the market a kick” rather than relying on the market to respond on its own (ibid, para. 3), and McConnell is quoted stating that “industry is not going to embrace [cybersecurity measures] unless they're forced to do it” (ibid, para. 4). This is quite a different framing compared to the harmonious relationship portrayed in the coverage of Google's partnership with the NSA, and relies more on emphasizing the urgency of the situation.

In this way it bears more similarities with McConnell's article which was published at around the same time.

The second article more closely follows the public-private partnership frame but does still contain the suggestion that private industry will need some cajoling, as is evidenced by the title which proclaims, “Legislation would *force* White House, private sector to collaborate in cyber-emergency” (Nakashima, 2010e, emphasis added). This need for the strong-arming of industry parallels the way the article frames President Obama's inaction, which has been seen in several other articles during and prior to the Google cyberattacks; it suggests that the legislation “is an attempt to prod the Obama administration and Congress to be more aggressive in crafting a coordinated national strategy for dealing with cyberthreats” (ibid, para. 2). Obama's strategy of careful consideration is compared negatively to that of previous president George Bush, as the article notes that “[d]espite an effort late in the Bush administration to create a national cybersecurity plan, the Obama administration's effort has been slowed by disputes over what roles the government and the private sector should play in protecting U.S. computer networks” (ibid, para. 5). Interestingly, this particular bill met with vehement opposition early on as the language suggested the president would be given a 'kill switch' to turn off the U.S. Internet in a national security emergency. This article stresses that such civil liberties objections are no longer a concern, emphasizing public-private collaboration as essential for cybersecurity progress (ibid, para. 7-8).

This close reading therefore highlights the extent to which the mainstream media reproduces dominant security discourses, and how this framing can facilitate the discussion and acceptance of related policy. By looking at the Google-China example as it develops over time, it is possible to see how the manipulation of the frames through which it is discussed shapes the public articulation of the issues, and thereby influences the debate.

Chapter 7.

Conclusions

Securitization as an Effect of and in the Media

This thesis contributes to a recent development in constructivist approaches to security studies which attempts to develop our understanding of how security threats are created, disseminated, and accepted. It has argued that attaching the national security label to issues of network security carries implications that are different to approaching the same questions through the frame of computer security, risk, or crime. The responses that such a frame legitimizes and even necessitates can restrict the freedoms of the populace, therefore it is of extreme importance to view discussions of cybersecurity as 'interested constructions' so as to ensure that the suggested response does not unnecessarily infringe on citizens' civil rights. As this thesis has shown, security professionals often emphasize the importance of the attribution and prevention of cyberattacks through the monitoring of network traffic (Clarke and Knake, 2010; McConnell, 2010). A powerful argument has been made for the development of this kind of monitoring, however its implementation and the agency who should be given responsibility for this task has been hotly debated. The success of these arguments is dependent on their acceptance by target audiences, and yet Copenhagen School scholars have barely touched on this aspect of securitization theory, focusing instead on the perlocutionary and illocutionary acts themselves (Balzacq, 2009, p. 11). Little attention is given to the question of which audiences are targeted, how they are reached, and the facilitating conditions necessary for an audience's acceptance of the speech act.

This thesis has attempted to develop securitization theory further using insights from communications research to posit that security arguments are transmitted to the general public through the media, which has an opportunity to influence public perception of cybersecurity as it is “the lens through which the public sees an issue” (Vultee, 2007, p. 3) and it “imparts to occurrences their public character as it transforms mere happenings into publicly discussable events” (Tuchman 1978, p. 3). The media can also provide a way for securitizing actors to rally support for their perspective, applying pressure to policymakers through their constituents, or even act as a medium through which policymakers communicate to one another (Robinson, 2001; Kingdon, 1995). This gives the media a degree of autonomy in and influence over the securitization process, as the way in which it chooses to frame an event can preclude or draw attention away from alternatives, making it more difficult for audiences (and especially lay audiences, given the highly technical nature of cybersecurity) to challenge a dominant perspective. However the media must also be seen as an audience itself that must be convinced by the securitizing move in order to frame its reporting using the same rhetoric.

While definitive conclusions on the influence of the media on a wider audience cannot be made, this thesis has shown that as an audience itself the media is predisposed to reflect dominant cybersecurity discourses and act as a space through which policymakers can call attention to specific security approaches. Therefore the media can be a useful way to track the evolution of cybersecurity policy debates. The data on media reporting has shown how public awareness of cyberthreats has grown in the U.S. since the 1990s. This is due in part to the huge growth in broadband penetration and the increase in reliance on networked computing throughout society, resulting in an actual increase in vulnerability as well as a hypothetical increase in the threats that are faced. While some news articles did draw attention to the civil liberties implications of proposed security measures, securitization was the dominant frame, and it is likely to have the greatest impact as “security is not a limited value, and so we are likely to want more of it regardless of any objective characterization of the situation” (Chandler, 2008). The possible sacrifice of some individual liberties such as privacy seems to be a satisfactory trade off in exchange for security from a threat which has been compared to the World Trade Centre attacks, the attack on Pearl Harbour, and a nuclear bomb. As the adage goes, you have nothing to fear if you have nothing to hide; whereas there is plenty to fear from a cyberattack, according to media reports.

The repetition of dominant frames in media reporting illustrates the rhetorical power of security. As the case study examined in this thesis demonstrates, despite the lack of proof that the Chinese government had sponsored or encouraged the cyberattacks against Google and other members of the U.S. technology industry, few of the news reports gave any attention to this fact, instead referencing established schemata in which China was the enemy and the aggressor, for example the Cold War and various recent clashes with the U.S. So effective was this framing that later in the year when the Wikileaks website posted diplomatic cables which confirmed that the Chinese government did have knowledge of and almost certainly ordered the cyberattacks, little attention was paid in the American press. The revelation appeared as a one line reference in several articles, and only two articles covered the implications of the Wikileaks reveal on the Google-China incident specifically. This is a clear sign of the success of the threat frame, as the revelation seems to be a confirmation of what was already assumed. However it also illustrates a flaw in the hope that the media can provide an outlet for policy dissensus, and can challenge dominant frames. As Kingdon noted in his research, the media has a short-term memory, and so new stories quickly replace old concerns (1995). The Google incident could not be revisited as it was 'old news', and the Wikileaks story itself was highly controversial. The veracity of these old claims was not part of the debate as the media framed and discussed it, and was therefore precluded by the discussion parameters.

Limited Effects: Considerations for Future Research

While this thesis has shown evidence for the acceptance of cybersecuritization in the media as an audience, and there is reason to believe that the repetition of these arguments in the media may have an effect on a wider audience, it was beyond the scope of this thesis to conduct empirical research into audience perception. However there is much scope for further research on the acceptance of securitizations by a wider audience—or to use Ciaran O'Reilly's term, within a 'critical mass' (2008). An issue does not become designated as a concern of national security purely due to a clever rhetorical strategy. Securitization theory rightly emphasizes the importance of the position held by the securitizing actor, but as Thierry Balzacq notes a major critique of the Copenhagen School is that it “overlooks the external context, the psycho-cultural orientation of the audience, and neglects the differential power between the speaker and the listener” (2005, p. 174). Because an audience accepts a securitization “based on what it knows about the world”, context is all-important (in Vultee, 2011, p.78). This thesis has used insights from limited effects research to develop the idea of external 'facilitating conditions' advanced by the Copenhagen School, and there is reason to believe the facilitating conditions specific to cybersecurity would allow media framing to have an impact on the acceptance of securitization by a wider audience. A brief comparison of the conclusions of this thesis with existing research in this area can perhaps explain why the media can be used to successfully securitize an issue in some cases but not in others, providing some important insights for future cybersecurity research.

Both Cirian O'Reilly and Fred Vultee apply Balzacq's insights to their research into audience perception, but they arrive at quite different conclusions. O'Reilly makes a case for the successful securitization of the Iraq War in the media, resulting in a military intervention despite a lack of popular support both nationally and internationally. However Vultee's empirical research into audience perception suggests that the presence of a securitizing discourse in the media may have little influence on the acceptance of a securitizing move. O'Reilly's research is similar to this thesis in that it examines the acceptance and repetition of the securitizing discourse in the media and makes the case that this would have an effect on a wider audience. Vultee uses a controlled experiment to test this theoretical influence of media frames on a general audience, and has found it to be lacking. O'Reilly emphasizes the role of the national climate within which arguments for the invasion of Iraq took place. He notes that “[t]he 9/11 attacks produced an inordinate level of national pride, sensitivity and public outrage within the United States which culminated in an atmosphere of hyper-patriotism” (2008, p. 66). Therefore he argues that the securitizing move involved “a concerted ‘hijacking’ of national feeling and fostering of hyper-patriotism, driven through the mainstream media, which played upon the 9/11 attacks and created an audience far more susceptible to securitization rhetoric” (2008, p. 67).

While Vultee similarly emphasizes the importance of the context in which the securitizing move occurs, he conceptualizes this differently. Quoting Balzacq, he argues that “threats can be securitized only when a securitizing move is enabled by a context—a frame—that “'selects' or activates certain properties of the concept, while others are concealed” (in Vultee, 2011, p. 81). Therefore it is clear that Vultee's examination of context relates closely to the frame—the frame provides the context. He develops this idea by looking at news 'channels', arguing that “[o]ne channel carries data, another a set of signals that put the data in social context: how the audience should feel about the data” (ibid, p. 82). This would once again seem to emphasize the importance of the speech act; while this interpretation does take into account the external factors or schemata that are recalled through the speech act, it does not consider the significance of the current social context into which the securitization is spoken. For example, Vultee's experiment used articles that “seemed likely to appear timely without reminding readers to a specific event toward which they might have already formed an opinion” (ibid, p. 84). This demonstrates a conscious avoidance of the social context into which the media speaks 'in the wild', and an attempt to limit the securitization to the frame itself. While this does allow for a greater control of influencing variables which is necessary for such a positivist method, it sacrifices the lived reality in which audiences receive and process news.

Vultee notes that “[a]s a cognitive cue, [a securitization] should act as a heuristic signal to reduce the intensity of processing—though any such effects are expected to be contingent on the audience's readiness to accept the frame” (2011, p. 84). This 'readiness' is essential to the securitization's success. O'Reilly argues that the hyper-patriotism that existed following the 9/11 attacks facilitated the invasion of Iraq soon after; the invasion was rhetorically figured as a response to the attacks. The relevant audiences were therefore ready to accept the argument, facilitated by the climate of fear in which it was made. By contrast, Vultee suggests that the same hyper-patriotism and fear of terrorism was used to shape audiences' perception of various news reports relating to immigration or border security, and to political violence. However the rhetorical link proposed in this study is far less direct and the study was conducted up to six years after the 9/11 attacks, meaning that, while referencing the terrorist attacks might highlight existing mental schemata, the lack of immediacy reduces the salience of the argument. The audience in Vultee's study was responding to his research in a very different social context, one in which they may not be 'ready' to accept this framing. While Vultee measured internal factors such as his participants' political orientation and attitude towards news media and current events, he attempted to control for external factors, except those referenced by the frame. Therefore his finding that the securitization had little effect on those who were not already predisposed to the speech act, might have been different had those participants been made 'ready' by external influences.

Rather than controlling for these external variables, this thesis has drawn from John Kingdon's agenda-setting theory (1995) in order to incorporate the influence of external context into an account of the steady increase in the significance of cybersecurity. In particular, the significance of a 'focusing event' is explored through the analysis of a recent, high-profile case study: the cyberattacks targeting Google and originating in China. A broad audience was 'ready' to accept the securitization of this particular incident because of the development of the cybersecurity field over the last ten years. The data illustrates a growing public awareness of cybersecurity threats which exploded in the last few years, and a review of the literature demonstrates the growing importance allocated to cybersecurity in military and intelligence sectors. As Vultee notes, a successful securitization occurs when “the right actor invokes the right threats under the right conditions to the right audience” (2011, p. 84). This thesis has argued that the Google-China incident provided just such an example.

The exploration of the development of cybersecurity in the media has shown that however convincing the securitization argument is, and however much media conventions bias journalists towards supporting official perspectives, there are many other factors which will influence likelihood of the acceptance and support of a securitizing frame by the media. For example the recurring critique of President Obama's inaction with regards to the development of cybersecurity policy, in contrast with the support seen in other sources for his cool-headed approach, is evidence of the fact that media framing is to an extent dependent on the internal socio-political structure of the news source, as well as external factors based on the socio-political climate in which the piece is written. The framing of the Google-China cyberattacks illustrates the strategies that securitizing actors employ in order to remove this element of choice from the media, and manipulate the way a cybersecurity event is framed. The careful timing of Google's announcement so that it coincided (apparently through no deliberate coordination) with Hillary Clinton's speech on Internet freedom made it difficult for the media to challenge U.S. security responses by suggesting that they endanger individual freedoms. The Chinese government had long been known for its attempts to control its citizens' access to information, while Clinton's speech served as a reminder of the Obama administration's commitment to freedom, and provided an opportunity to openly challenge Chinese censorship policies. The framing of this particular incident changed the terms of the cybersecurity debate, so that civil liberties were no longer a necessary casualty of increased security, but rather security measures were necessary to safeguard Internet freedom.

Questioning Extraordinary Measures

The example explored in this thesis also highlights the extraordinary response that is justified by the securitizing move. In O'Reilly's research, the invasion of Iraq was part of a response characterized as the 'war on terror' that was justified as a way to prevent a repeat of any attack similar to the one carried out on the World Trade Centre. As has been noted, this clear causal link was missing from Vultee's research; however this does not mean that the extraordinary response must be proposed alongside the security incident. In fact, this thesis demonstrates that the potential for questioning these responses is often so difficult because emergency responses *are not* proposed alongside the threat frame itself. As the Google-China case study shows, after the story of the cyberattacks broke, calls for action were made and the U.S. aligned itself with freedom. However it was not until a month later that policy suggestions were publicly made, and it was two months after the incident that Google officially responded. By this time the threat frame through which the incident was portrayed was already long-established and the incident had become a schema which could be referenced later in policy discussions as evidence of the need for a certain type of action.

One element of the proposed response involved the collaboration of the public and private sectors in an effort to enhance security. As we have seen, the need to safeguard privately owned cyber and critical infrastructure has long been a central concern of cybersecurity discussions, however efforts by the government to manage the security of industry have been strongly resisted, due in part to a particularly American distaste for 'big government' and a belief that the market would dictate the appropriate response. Google's voluntary disclosure of the breach of its digital infrastructure was a watershed moment, breaking the unspoken industry code not to admit to failings in security that could threaten customer data and spook shareholders. In addition, the company then notified the U.S. government, with which it enjoys a close relationship, and then invited the National Security Agency to assist in the investigation of the breach, and in improvements to the company's security. Therefore this incident provides a fine example of the public-private collaboration that government has been working hard to encourage, while the reliance on the skills of NSA highlights the potential success of a particular set of securitizing actors who have been promoting the agency as the frontrunner in the cybersecurity turf war.

Viewed in a wider context, the Google-China example can be seen as a first success in a longer-term securitizing move. Mike McConnell's *Washington Post* article illustrates this context nicely, as he lists a string of so-called 'cyber-battles' that are evidence of the larger cyberwar in which the U.S. is embroiled. Besides the Google cyberattack, he also notes that

> the security firm NetWitness reported that more than 2,500 companies worldwide were compromised in a sophisticated attack launched in 2008 and aimed at proprietary corporate data. Indeed, the recent Cyber Shock Wave simulation revealed what those of us involved in national security policy have long feared: For all our war games and strategy documents focused on traditional warfare, we have yet to address the most basic questions about cyber-conflicts. (McConnell, 2010, para. 4)

The 'Cyber Shock Wave' simulation to which he refers was a CNN two-hour prime-time special; a televised simulation of a 'situation room' that showed the 'government' responding to a cyberattack on U.S. critical infrastructure as it unfolded, with the roles played by current and former government officials. Richard Grusin's analysis of the broadcast was that it was meant to “scare the American public so that they would be willing to accept the imposition of even more draconian security powers for the US government”, and he suggested that, viewing the show as part of “a continued premediation campaign distributed across print, televisual, and networked media, a campaign that is in full swing and appears to be heating up, Cyber Shock Wave might have some small effect on modulating individual and collective affect” (2010, para. 1). Later that year, this campaign was vindicated by the discovery of the Stuxnet, a virus that affected Siemens' supervisory control and data acquisition (SCADA) system—the type of system that controls critical infrastructure. Stuxnet was likely designed to target the Siemens equipment used in Iranian uranium enrichment infrastructure (Falliere et al., 2011).

Securing Freedom

In conclusion, it has been shown that cybersecurity has been successfully placed on the security policy agenda after a long-term securitizing move, and that the media is an ideal space through which to track the development of these security arguments. The media can both be seen as an audience itself, and a functional actor through which security professionals seek to convince a wider audience of the necessity of their particular brand of security. This thesis has demonstrated the importance of external facilitating conditions in this effort, and particularly of a 'focusing event' that gives legitimacy to otherwise hypothetical threat frames. The Google-China incident was a perfect example of such an event. By understanding that the media is an audience itself, security professionals were able to use journalistic conventions to manipulate the framing of this event so as to change the terms of the cybersecurity debate. Rather than approaching the issue along the usual adversarial lines, increased control and surveillance of cyberspace were portrayed not as a threat to civil liberties, but rather as a necessary measure in order to secure freedom.

Print References

Abbate, J. (1999). Inventing the Internet. Cambridge, Mass: MIT Press

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

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

Arnett, E.H. (1992). Welcome to Hyperwar. The Bulletin of the Atomic Scientists, 48(7), p. 14-21.

Arquilla, J. and Ronfeldt. D. (1993). Cyberwar is Coming! Santa Monica, CA: RAND Corporation. Accessed on January 26, 2010 from http://www.rand.org/pubs/reprints/RP223.

Austin, J. (1975). How to do things with words. Cambridge, MA: Harvard University Press

Balzacq, T. (2005). The three faces of securitization: Political agency, audience and context. European Journal of International Relations, 11, 171-201 doi: 10.1177/1354066105052960

Balzacq, T. (2009). Constructivism and Securitization Studies. Retrieved on October 11, 2011 from http://graduateinstitute.ch/webdav/site/developpement/shared/developpement/cours/E777/Securitization_Balzacq.pdf

Bendrath, R. (2003) The American cyber-angst and the real world – Any link? In Latham, R. (Ed.). Bombs and bandwidth: The emerging relationship between information technology and security, (pp. 49-73). New York: The New Press.

Berkowitz, B. (2003). The new face of war: How war will be fought in the 21st century. New York: Free Press.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. Alternatives 27, 63-92.

Bigo, D. and Anastassia Tsoukala. (2008). Terror, insecurity and liberty: Illiberal practices of liberal regimes after 9/11. New York: Routledge.

Bijker, W.E. (2006). The vulnerability of technological culture. In H. Nowotny (Ed.), Cultures of Technology and the Quest for Innovation. (52-69). New York: Berghan Books.

Bremmer (2010, March 22). China vs America: fight of the century. Prospect Magazine (169)

Brito, J. and Tate Watkins. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center, George Mason University Working Paper No. 11-24, April 2011. Accessed on June 28, 2011 at http://mercatus.org/sites/default/files/publication/WP1124_Loving_cyber_bomb.pdf

Buzan, B., Wæver, O. And de Wilde, J. (1998) Security: A new framework for analysis. Boulder: Lynne Rienner

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

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

Buzan, B. and Hansen, L. (2009) The evolution of international security studies. Cambridge Cambridge, UK: University Press

Chandler, J. (2008). Privacy versus national security: Clarifying the trade-off. In I. Kerr, V. Steeves and C. Lucock (Eds.), On the Identity Trail: Anonymity, privacy and identity in a networked society (pp. 121-138) Oxford: Oxford University Press. Retrieved from June 28, 2011 at http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_07.pdf

Clark, W.K. and Levin, P.L. (2009) Securing the information highway: How to enhance the United States' electronic defenses. Foreign Affairs. 88(4), 2-10

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

Clinton, H. (2010, January 21). Remarks on Internet freedom. Speech presented at the Newseum, Washington D.C. Accessed on July 20, 2010 at http://www.state.gov/secretary/rm/2010/01/135519.htm

Clinton, W.J. (1998, May). Presidential Decision Directive 63. Government Printing Office: Washington, DC

Debrix, F. (2001). Cyberterror and Media-Induced Fears: The Production of Emergency Culture. Strategies, 14(1), p. 149-168. DOI: 10.1080/10402130120042415

Deibert, R.J. (2003) Black code: Censorship, surveillance, and the militarisation of cyberspace. Millennium 32 (3), 501-30.

Deibert, R.J., Palfrey, J.G., Rohozinski, R., and Zittrain, J. (Eds.). (2010). Access Controlled: The shaping of power, rights, and rule in cyberspace. Cambridge: MIT Press

Department of Homeland Security. 2003. The national strategy to secure cyberspace. The President's Critical Infrastructure Protection Board: Washington, D.C. Accessed on June 28, 2010 at http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Der Derian, J. (2001) Virtuous war. Boulder, Colorado: Westview Press.

Der Derian, J. (2008). Critical encounters in international relations. International Social Science Journal, 59(191), 69 – 73.

Dunn Cavelty, M. (2007a). Cyber-terror–Looming threat or phantom menace? The framing of the US cyber-threat debate. Journal of Information Technology & Politics, 4(1) 19-36. doi:10.1300/J516v04n01_03

Dunn Cavelty, M. (2007b). Cyber-security and threat politics: U.S efforts to secure the information age. New York: Routledge.

Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. New York: Routledge.

Edwards, P.N. (1996). The closed world: computers and the politics of discourse in Cold War America. Cambridge, Mass: MIT Press

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

Eriksson, J. and Giacomello, G. (2007). Introduction: Closing the gap between international relations theory and studies of digital-age security. In J. Eriksson and G. Giacomello (Eds.), International Relations and Security in the Digital Age (pp. 1-29). New York: Routledge.

Falliere, N., Murchu, L.O., and Chien, E. (2011). W32.Stuxnet Dossier. Accessed on October 6, 2010 from http://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Fairclough, N. (1989). Language and power. London: Longman.

Fischer, F. (1990). Technocracy and the politics of expertise. Newbury Park, Calif: Sage Publications

Fiveash, K. (2011, June 6) Google acting as a 'political tool', says China. The Register. Accessed on August 2, 2011 at http://www.theregister.co.uk/2011/06/06/china_gmail_hacking_claims_damage_google_business/

Frye, E. (2002). The tragedy of the cybercommons: Overcoming fundamental vulnerabilities to critical infrastructures in a networked world. The Business Lawyer, 58, p. 349-382

George, A. (1980). Presidential decision making in foreign policy: The effective use of information. Boulder, CO: Westview Press

Giddens, A. (2002) Runaway world : How globalisation is reshaping our lives. London : Profile

Gramsci, A. (2005). Selections from the Prison Notebooks. (Q. Hoare and G. Smith, Eds. and Trans.). New York: International Publishers.

Gray, C. H. (1997). Postmodern war: The new politics of conflict. New York: Guildford Press.

Gray, C.H. (2005). Peace, war, and computers. New York: Routledge

Grusin, R. (2010, February 25). Cyber Shock Wave--Fearmongering on CNN [Web log comment]. Retrieved from http://premediation.blogspot.ca/2010/02/cyber-shock-wave-fearmongering-on-cnn.html

Haggerty, K. and Ericson, R. (2006). The new politics of surveillance and visibility. Toronto: University of Toronto Press

Hammond, P. and Herman, E. (Eds.). (2000). Degraded capability: The media and the Kosovo crisis. London: Pluto Press

Hansen, L. and Nissenbaum, H. (2009) Digital disaster, cyber security, and the Copenhagen School. International Studies Quarterly, 53, p. 155–1175

Hayes, A.S., Singer, J. B., and Ceppos, J. (2007). Shifting Roles, Enduring Values: The Credible Journalist in a Digital Age. Journal of Mass Media Ethics, (22)4, pp. 262-279. DOI: 10.1080/08900520701583545

Herman, E. (1993). The media's role in US foreign policy. Journal of International Affairs, 47(1), 23-45

Herman, E. and Chomsky, N. (1988). Manufacturing consent. New York: Pantheon

Hillsman, R. (1987). The politics of policy making in defense and foreign affairs. Englewood Cliffs, NJ: Prentice-Hall

Hughes, R. (2007). Bits, Bytes and Bullets. The World Today, (63)11, p. 20-22

Huysmans, J. (2004). Minding exceptions: The politics of insecurity and liberal democracy. Contemporary Political Theory, 3, 321–341

Iyengar, S. (1991). Is anyone responsible? Chicago: University of Chicago Press

Johnson, T.J. and Kaye, B.K. (2004). Wag the Blog: How Reliance on Traditional Media and the Internet Influence Credibility Perceptions of Weblogs Among Blog Users. Journalism & Mass Communication Quarterly, 81, p. 622- 642 DOI: 10.1177/107769900408100310

Joint Chiefs of Staff. (1996). Information Warfare: A strategy for peace... the decisive edge in war. USGPO Doc. D 5.2:IN3, 1997, http://handle.dtic.mil/100.2/ada318379.

Kahneman, D and Tversky, A. (1984). Choice, values, and frames. American Psychologist, 39, 341-350. doi:10.1057/palgrave.cpt.9300137

Katz, E. and Lazarsfeld, P.F. (1955). Personal influence. New York: The Free Press.

Kingdon, J.W. (1995). Agendas, alternatives, and public policies. New York: Longman

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. New York: United Nations. Retrieved August 2, 2011 at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Langevin RJR et al. (2009) Securing cyberspace for the 44th presidency. Washington, D.C.: Center for Strategic and International Studies.

Lasswell, H. D. (1948). The structure and function of communication in society. In L. Bryson (Ed.) The Communication of Ideas (pp. 117-130). Urbana, IL: University of Illinois Press

Lessig, L. (2000). Codes and other laws of Cyberspace. New York: Basic Books.

Lyon, D. (2003). Surveillance after September 11. Cambrigde, UK: Polity Press

MacDonald, M. (2008) Securitization and the construction of security. European Journal of International Relations, 14, 563-587. doi: 10.1177/1354066108097553

National Security and Homeland Security Councils. 2009. Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. Executive Office of the President of the United States: Washington, DC. Accessed on 28 June, 2011 at http://purl.access.gpo.gov/GPO/LPS118258

Neubauer, R. (2011). Neoliberalism in the information age, or vice versa? Global citizenship, technology, and hegemonic ideology. TripleC 9(2), 195-230

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

Noble, D.F. (1977). America by design: science, technology, and the rise of corporate capitalism. New York: Knopf

O'Reilly, C. (2008). Primetime patriotism: News media and the securitization of Iraq. Journal of Politics and Law 1(3), 66-72

Pan, Z. and Gerald Kosiki. (1993). Framing analysis: An approach to news discourse. Political Communication, 10, 55-75

Parsons, C. (2012, February 28)The Issues Surrounding Subscriber Information in Bill C-30 [Web log comment]. Retrieved from http://www.christopher-parsons.com/blog/technology/the-issues-surrounding-subscriber-information-in-bill-c-30/

President’s Commission on Critical Infrastructure Protection. (1997) Critical foundations: protecting America’s infrastructures. The Commission: Washington, D.C. Accessed on June 28, 2011 at http://www.fas.org/sgp/library/pccip.pdf

Rattray, G.J. (2001). Strategic warfare in cyberspace. Cambridge, Mass: MIT Press

Robinson, P. (2001). Theorizing the influence of media on world politics: Models of media influence on foreign policy. European Journal of Communication, 16, 523-544. DOI: 10.1177/0267323101016004005

Rowland, W. (2006). Spirit of the Web. Toronto: Thomas Allen Publishers

S. 3480--111th Congress: Protecting Cyberspace as a National Asset Act of 2010. (2010). InGovTrack.us (database of federal legislation). Retrieved January 14, 2012, from http://www.govtrack.us/congress/bill.xpd?bill=s111-3480

Saco, D. (1999). Colonizing cyberspace: National security and the Internet in Jutta Weldes, Mark Laffey, Hugh Gusterson, and Raymond Duvall (Eds.), Cultures of insecurity: States, communities, and the production of danger. Minneapolis: University of Minnesota Press.

Schiller, D. (1996). Theorizing communication: A history. New York: Oxford University Press

Schneier, B. (2008). Schneier on security. Indianapolis, IN: Wiley Publishing

Schwartau, W. (2012, July) Winn Schwartau predictions and more. Retrieved December 12, 2012 from winnschwartau.com/assets/docs/WinnPredictsJuly12.pdf

Singer, P.W. (2003). Corporate Warriors: The rise of the privatized military industry. Ithaca, New York: Cornell University Press.

Sterling, B. (1992). The Hacker Crackdown. New York: Bantum Books

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. European Journal of International Relations, 13, 357-383. doi: 10.1177/1354066107080128

Smythe, D. (1986). On the political economy of C3I, in Becker, J., Hedebro, G. And Paldin, L. (Eds.), Communication and domination: Essays to honor Herbert I. Schiller. New Jersey: Ablex Publishing Corporation.

Tuchman, G. (1978). Making news: A study in the construction of reality. New York: Free Press.

Vultee, F. (2007). Securitization as a theory of media effects: The contest over the framing of political violence (Doctoral dissertation). Retrieved from University of Missouri at https://mospace.umsystem.edu/xmlui/bitstream/handle/10355/4792/research.pdf

Vultee, F. (2011). Securitization as a media frame:What happens when the media 'speak security'. In Balzaqc, T. (Ed.), Securitization theory: How security problems emerge and dissolve. New York: Routledge

Van Eeten, M. and Bauer, J. (2009). Emerging threats to Internet security: Incentives, externalities and policy implications. Journal of Contingencies and Crisis Management 17(4), 221-232

Van Loon, J. (2002) Risk and technological culture : Towards a sociology of virulence. New York : Routledge

Weldes, J. et. al. (1999). Introduction: Constructing insecurity in Weldes, J. Laffey, M. Gusterson, H., and Duvall, R. (Eds.), Cultures of Insecurity (1-35). Minneapolis, MN: University of Minnesota

Whyte, J.O. (2010). The military audience commodity: Reopening the blindspot debate (Masters dissertation). Retrieved from https://theses.lib.sfu.ca/thesis/etd6360

Winner, L. (1977). Autonomous technology: Technics-out-of-control as a theme in political thought.
Cambrige, M.A.: MIT Press.

Zaller, J.R. (1992). The nature and origins of mass opinion. New York: Cambridge University Press

Zittrain, J. (2008). The future of the Internet and how to stop it. New Haven, CT: Yale University Press

Media References

Acohido, B. (2010, February 4). Cybersecurity looks hot in 2010; Attacks on Google make security vendors good bet. *USA Today*, p.1B

Acohido, B. and Swartz, J. (2010, January 13). Censorship may spur Google to exit China; Tech giant also points to cyberattacks as an issue. *USA Today*, p. 1B

Areddy, J.T. (2010, January 13). Levi's faced earlier challenge in China; Jeans company walked out 17 years ago, but today has 501 stores. *Wall Street Journal Online*, accessed on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Back, A. and Vascellaro, J. (2010, January 14). White House, Beijing joust over censorship; Microsoft says hackers exploited a vulnerability in its Internet browser in attack against Google, others. *Wall Street Journal Online*, retrieved on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Bolton, J. (2010, January 21). Google didn't kowtow and neither should you; The company is only insisting on reciprocal fair dealing--something that is in America's interest, too. *Wall Street Journal Online*, accessed on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Cha, A.E. and Nakashima, E. (2010, January 14). Google China cyberattack part of vast espionage campaign, experts say. *The Washington Post.* Accessed July 20, 2011 at http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html

Cohen, R. (2010, March 30). Google's lonely stand. *The Washington Post*, p. A25

Dean, J. (2010, January 13). Ethical conflicts for firms in China. *Wall Street Journal*, p. A6, retrieved on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Fishman, T.C. (2010, January 21). How Google mirrors China; The company and the country interact with the world according to the rules they have written. *USA Today*, p.11A

Goldsmith, J. (2010, February 1). Can we stop the cyber arms race? *The Washington Post*, p. A17

Gorman, S. (2010a, January 14). Web is new front among Cold War foes; Attacks against multinational corporations would represent a significant expansion of targets beyond the military. The Wall Street Journal Online, retrieved on February 22, 2012 at http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Gorman, S. (2010b, January 21). U.S. news: Web access is new Clinton Doctrine. *Wall Street Journal*, p. A.3.

Gorman, S. and Barnes, J. (2011, May 31) Cyber combat: Act of war. *Wall Street Journal*. Accessed on August 2, 2011 at http://online.wsj.com/article/SB10001424052702304563104576355623135782718.htm

Google. (2010, January 12). *Official Blog*, "A new approach to China". Retrieved on June 27, 2012 from http://googleblog.blogspot.ca/2010/01/new-approach-to-china.html

Helft, M. (2010, January 13). Google's threat would mean giving up a lucrative market. *The New York Times*, p. A3

Helft, M. and Markoff, J. (2010, January 14). In Google's rebuke of China, focus falls on cybersecurity. *The New York Times*, p. A1

Hernandez, J.C. (2010, March 25). Google calls for action on web limits. *The New York Times on the Web*, accessed on February 22, 2012 from http://www.nytimes.com/2010/03/25/technology/25google.html

Jacobs, A. and Helft, M. (2010, January 13). Google may end venture in China over censorship. *The New York Times*, p. 1A

Kristof, N.D. (2010, January 14). Google takes a stand. *The New York Times*, p. A37

Kang, C. (2010, January 22) Clinton calls for Internet freedom; She wants China to probe Google attack, looks to bar censorship. *The Washington Post*, A14

Kravets, D. (2010, January 29). Courts, Congress shun addressing legality of warrantless evesdropping. *Wired Magazine*, accessed on July 16 2010 at http://www.wired.com/threatlevel/2010/01/legality-of-warrantless-eavesdropping/

Landler, M. and Wong, E. (2010, January 23). China says Clinton harms relations with criticism of Internet censorship. *The New York Times*, p. A4.

Levy, S. (1997, June 1). The Day the World Shuts Down, in *Newsweek*. Accessed on March 16, 2012 at http://www.thedailybeast.com/newsweek/1997/06/01/the-day-the-world-shuts-down.html

Levy, S. (1994). “The Battle of the Clipper Chip.” New York Times Magazine, June 12, 44-51, 60, 70

Markoff, J. (2010a, January 20). New claim of evidence on Google's China case. *The New York Times*, p. B4

Markoff, J. (2010b, February 5). Google Asks Spy Agency to Look Into Cyberattacks. *The New York Times*, p. A6

Markoff, J., Sanger, D. and Shanker, T. (2010, January 26). In digital combat, U.S. finds no easy deterrent. *The New York Times*, p. A1

McConnell, M. (2010, February 28). To win the cyber-war, look to the Cold War. *The Washington Post*, p. B1

Milbank, D. (2010, January 6). Obama's review mirror. *The Washington Post*, p. A2

Nakashima, E. (2010a, February 4). “Google to enlist NSA to ward off attacks” in *The Washington Post*

Nakashima, E. (2010b, January 16). U.S. plans to issue official protest to China over attack on Google. *The Washington Post*, p.A4

Nakashima, E. (2010c, January 3). Questions stall Pentagon computer defenses; Officials are addressing concerns about mission and privacy issues. *The Washington Post*, p. A4

Nakashima, E. (2010d, February 4). Google to enlist NSA to ward off attacks; Firm won't share user data, sources say, but deal raises issue of privacy vs. security. *The Washington Post*, p. A1

Nakashima, E. (2010e, March 17). Legislation would force White House, private sector to collaborate in cyber-emergency. *The Washington Post*, p. A4

Nakashima, E. and Cha, A.E. (2010, January 15). Search giant vs. global powerhouse a tough fight for U.S. to referee. *The Washington Post*. Accessed on August 10, 2012 from http://www.washingtonpost.com/wp-dyn/content/article/2010/01/14/AR2010011404077.html

Nakashima, E., Mufson, S. And Pomfret, J. (2010, January 13). Google threatens to leave China; Hackers attack networks of major companies, e-mail accounts of activists. *The Washington Post*, p. A01

Peaple, A. (2010, January 13). Google's watershed moment in China. *The Wall Street Journal Online*, retrieved on February 22, 2012 at http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Portilho-Shrimpton, T. (2008, August 17). Battle for South Ossetia fought in cyberspace. *The Independent*. Retreived on January 13, 2010 from http://www.independent.co.uk/news/world/europe/battle-for-south-ossetia-fought-in-cyberspace-899772.html

Sanches, J. (2009, April 6). Senators introduce bill to federalize cybersecurity. *Arstechnica*. Retrieved on December 12, 2012 from http://arstechnica.com/tech-policy/2009/04/sens-introduce-bill-to-federalize-cybersecurity/

Sanger, D. and Markoff, J. (2010, January 15). U.S. Treads Lightly in Wake of Google's Loud Stance on China. *The New York Times*, p. A1

Schultz, S. (2005, December 28). Calls made to strengthen state energy policies. *The Country Today*, pp. 1A, 2A.

Shachtman, N. (2010, June 3). The Dangers of Turning Spies into Generals (and Vice Versa) in *Wired Magazine*. Accessed on March 14, 2012 at http://www.wired.com/dangerroom/2010/06/the-dangers-of-turning-spies-into-generals-and-vice-versa/

Solomon, J., Johnson, I. and Dean, J. (2010, January 14). U.S. Holds Fire in Google-China Feud. *Wall Street Journal Online*, retrieved on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Stone, B. (2010, January 21). 5 Senators urge Clinton to expedite aid for groups fighting Internet censors. *The New York Times*, p. 10

USA Today. (1995, October 24). One little change could end cyber-security woes . . . *USA Today*, p. 12A

USA Today. (1996, December 26). Privacy takes another hit from new computer rules. *USA Today*, p. 8A

Vascellaro, J.E., Dean, J. and Gorman, S. (2010, January 13). Google warns of China exit over hacking; Cyber attack targeted as many as 34 firms, email of human-rights activists; Investigators probe link to Chinese government. Wall Street Journal Online, retrieved on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Vascellaro, J.E., and Solomon, J. (2010, January 14). Yahoo was also targeted in hacker attack. *Wall Street Journal Online*, accessed on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Wall Street Journal. (2010a, February 2). China's human-rights hacking; Attempts to silence critics extend beyond the mainland's borders. *The Wall Street Journal Online*, accessed on February 22, 2012 at http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237957873?accountid=13800

Wall Street Journal. (2010b, January 21). The Clinton Internet Doctrine; Kudos to the State Department's campaign to preserve and expand Internet freedom around the world. *Wall Street Journal Online*, accessed on February 22, 2012 from http://proxy.lib.sfu.ca/login?url=http://search.proquest.com/docview/237936273?accountid=13800

Washington Post (2010c, February 24). Nation Digest. *The Washington Post*, p. A3

Wines, M. (2010, January 15). Far-ranging support for Google's China move. *The New York Times on the Web*, accessed on February 22, 2012 from http://www.nytimes.com/2010/01/15/world/asia/15china.html

Wong, E., Ansfield, J. And Lafraniere, S. (2010, January 21). China paints Google issue as not political. *The New York Times*, p. 10

Wright, L. (2008, January 21). The Spymaster. *The New Yorker.* Accessed on July 31, 2012 at http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright?printable=true

Zuckerman, M.J. (1996a, July 17). Cybersecurity plan labeled 'urgent' Clinton administration sees role for both public, private sectors on new commission. *USA Today*, p. 2A

Zuckerman, M.J. (1996b, July 16). U.S. seeks to secure cyberspace. *USA Today*, p. 1A

Zuckerman, M.J. (1996c, June 5). Feds ready anti-terror cyberteam. *USA Today*, p. 1A