Borders to Borderless:
An Analysis of the Social Construction of the US Securitization Agenda (2006-2010)

Dané Smith

Dané Smith, 24, is a South African national raised in the Sultanate of Oman with a Honours Degree in Bachelor of Social Science from Monash University. Her dissertation analyzed the social construction of US securitisation agendas across the twenty-first century. She is currently working in Muscat, Oman as an English Lecturer at the Oman Medical College. She has been accepted as a PhD candidate at Monash University starting March 2016 where she will be specializing into the migration-security nexus and conflict-resolution in the Middle East. Her interests include security and development, migration, peacebuilding, conflict resolution, security studies, transnational studies, foreign intervention and the Middle East region. dsmith92@gmail.com

Abstract

This study explores the relative contributions of state rhetoric, the public sphere and corporate elite interests towards the construction of the 2010 US National Security Strategy (NSS). Interpreted thusly, the evolution in the US securitisation agenda illustrates the social construction of US securitisation strategy as a national artefact seemingly informed by local interests but framed within international uncertainty. Exploring the relative contributions of state rhetoric, the public sphere and corporate elite interests thusly, indicates that different threat matrixes emerge from the social forces that propel the 2010 NSS into being. The research, in accordance with its approach, finds that the focus of securing the threat of risk to national interests and assets within international uncertainty, results in the form of US securitisation strategy not fully realising its function of securitisation. Through deliberating on how and why particular threats are prioritised above others to the nation-state, this article seeks to motivate further research into the social construction of policy priorities to better understand how and why threat matrixes shift in the 21st Century.

Keywords

Security studies, National Security Strategy, US securitisation, 9/11 attacks, Iraq invasion, Cybersecurity, Social constructivism, Technological determinism

Originally published in Volume 29 (March 2016), pp. 229–246. Corrected November 2026: volume and issue numbering.
https://doi.org/10.22151/politikon.29.14

FRAMING US SECURITISATION

Since the 9/11 attacks, US securitization strategy has evolved from prioritizing the territorial security of its borders, to more recently, prioritizing the securitization of risk and vulnerabilities toward US interests and assets within ungovernable constructs, such as cyberspace. Needing to evolve to adapt to new environments and threat matrixes, can be seen to have pushed US securitization strategy into an ambiguous space with several security dilemmas. One such dilemma is that, while evolutionary national security frameworks provide security, they also create insecurity because the threats they seek to secure are not necessarily identifiable or tangible. In order to avoid a continuation of such insecurity, this article attempts to unpack the social processes that inform national security frameworks in hope of informing how processes of securitization risk creating more insecurity.

Within security studies, securitization refers to the politicization of an identified issue into an existential threat deserving of extraordinary measures typically not within the realm of everyday political procedure (Liotta 2005: 51). The NSSs of 2002, 2006 and 2010 are representative of particular phases of securitization that are pushed into action through shifting threat matrixes. The 2002 NSS placed priority on a retaliatory security agenda against existential threats. The dominant discourses that contributed to the emergence of the 2002 NSS, established the necessary foundation for the emergence of the 2006 NSS. The continuities between the 2002 and 2006 NSSs are evident in the 2006 NSS's evaluation of the successes and failures of meeting the 2002 NSS objectives (The White House 2006). Notwithstanding the similarities between the 2002 and 2006 NSSs, there is a fundamental shift in the form of US securitization following the March 2003 invasion of Iraq (The White House 2006). The Iraq invasion was framed as a necessary measure to circumvent the existential threat posed by rogue states and terrorist networks beyond US national borders (Taylor 2006: 392). The Iraq invasion marks a pinnacle moment in 21st century US securitization, where the securitization strategy set by the 2002 NSS is transformed from a retaliatory to a pre-emptive stance; opening up the agenda for securitization within national borders and abroad simultaneously (Klippstein 2003: 273).

The NSSs of 2006 and 2010 are underpinned by similar concerns as per the securitization of US borders and national interests from transnational terrorist 'attacks' (The White House 2006; 2010). The possibility of terrorist attacks is used to rationalize the US's evolving securitization strategy across the NSSs, beginning with the securitization of national borders and moving most recently into the securing of US interests within ungovernable constructs, such as cyberspace (The White House 2010: 8). The representation of cyberspace within the 2010 NSS is indicative of the incorporation of risk as threat in the form of the vulnerabilities posed by asymmetrical attacks against US interests and assets (The White House). The 2006 and 2010 NSSs, point to the possibility that contemporary dynamics require states to secure spaces beyond their borders in addition to securing their borders, so as best to secure the territory and interests of the states concerned. In the 2006 NSS, for instance, President Bush refers to the increasing emergence of unfamiliar security concerns beyond US borders as by-products of the global age; concerns that do not necessarily fall into the realm of traditional security concerns (The White House 2006: 47).

Without understanding both why and how securitization strategy is pushed into action, national security frameworks are exposed to the vulnerability of the form of securitization not meeting its

function (Waever 1995). Embedded in a qualitative design within a social constructivist paradigm, the social processes that have allowed for particular threat matrixes to emerge between 2006 and 2010 in US securitization are investigated, in order to allow for better suited national security frameworks to be designed vis-à-vis the global age.

In order to comprehensively examine the social forces that propel the NSS into action, it is of particular importance to define the sources of such forces. In this respect, three major stakeholder groups are identified; the state, the public sphere and the corporate elite. The selection of these groups is premised on their significant role in policy formation (Schneider 1991, 27-30). The state refers to government bodies whose rhetoric constitutes disclosures to the public, such as Presidential speeches and state agency reports (Howlett 1992: 275). The public sphere constitutes a culmination of US-based media and polling organizations. The media cuts across a wide political spectrum from more conservative bias and liberal bias. Public sphere discourse is considered to be representative of opinions held by actors who are neither members of significant economic actors nor representatives of government (Holborn 2004: 575). Corporate elites refer to private economic actors who are members of, or act in the interest of influential corporate actors (Holborn 2004: 573). Their interests are most commonly illustrated via lobby group position papers and state-private sector partnerships. These understandings of state rhetoric, public sphere discourse and corporate elite interests inform the exploration into the narratives that inform the emergence of the 2010 NSS as a means of demonstrating the shifting nature of US securitization in the 21st century.

To examine the broader evolutionary nature of how US securitization strategy has been propelled into action, the theory of technological determinism is applied directly to understanding the emergence of the 2010 NSS. In accordance to Marshall McLuhan's Tetrad of Media Effects, a set of specific questions can be posed to illuminate the form and function of technological and institutional innovations within complex societies (Stamps 2001: 147). McLuhan's Thesis on Media Effects argues that the culture of a society is directly, yet imperceptibly affected by the technologies and their advancements that permeate that society (Ibid).

The questions posed as per the 2010 NSS content in order to unpack, and understand the narratives that pushed risk as a threat forward as a priority in contemporary US securitization agenda are:

i) **ENHANCES**: What does the NSS enhance?

ii) **OBSOLESCES**: What does the NSS position as less urgent in securitization strategy?

iii) **RETRIEVES**: What does the NSS retrieve that was dismissed in the preceding securitization strategy?

iv) **REVERSES**: What does the NSS turn into when pushed to extremes?

Responding to questions about the form and function of US securitization allows for an analysis and exploration of the construction of US security strategies and the forces that propel them into action, so as to better inform future policy. The space constraints affiliated with this article prevents a thorough historical discussion of the shifting US securitization threat matrixes. Through

expanding particularly on the social construction of the 2010 NSS, this article hopes to offer a new perspective to analyzing security policy agenda.

CONTEMPORARY US SECURITISATION: THE RISK IS THE THREAT

Following the 2006 NSS, US securitization emerged increasingly focused on the securitization of risk. Risk, as depicted by the 2010 NSS, constitutes possible asymmetric attacks with transnational reach against US national interests and assets. The risks that are identified as existential threats to US national security are framed within US securitization to be affiliated with ungovernable constructs such as biological threats, stagnation of global economic flows, the lack of adherence to universal values and unregulated information and communications technologies (ICTs) (The White House 2010: 2).

The space constraints affiliated with this article prevents a comprehensive discussion of all the ungovernable constructs identified in the 2010 NSS and the risks they pose to US national security. This article, in hope of opening up a space for more debate on the insecurity that may be created by securitization measures, will focus its deliberations particularly on the construct of cybersecurity as a representation of the securitization of risk as a top national security priority. Elaborating on how and why cybersecurity has emerged as a top national security priority will also illustrate the broader shift that has taken place in US securitization from prioritization of pre-emptive securitization - as illustrated by the 2006 NSS - to prioritizing the securitization of risk. The chapter will elaborate on the precedence the 2010 NSS places on cybersecurity, followed by deliberating on the social construction of risk as central to the threat matrix. Such deliberation will allow for the development of a better understanding of the broader securitization of risk that features across US securitization.

The Discourse of ' Risk is the Threat' in the 2010 NSS

The securitization of risk within national security discourse is evidenced by continual references made in the 2010 NSS, that national security strategies must accommodate risks posed by globalization through improving its comparative position of American leadership in world affairs. The 2010 NSS instructs that the best manner in which the comparative position of America can be ensured in a globalized world is through the management and mitigation of risk as a by-product of the global age:

> [I]n a world of greater interconnection – a world in which our prosperity is inextricably linked to global prosperity, our security can be directly challenged by developments across an ocean, and our actions are scrutinized as never before (The White House 2010: 2).

The call for the securitization of risk by the 2010 NSS, illustrates a shift in security discourse from prioritizing pre-emptive securitization– as advanced by the 2006 NSS - to prioritizing the securitization of risk. Rather than focusing on securing physical borders, the 2010 NSS advocates the securitization of US assets directly influenced by transnational constructs such as intellectual property rights, which are safeguarded or exploited in cyberspace.

The 2010 NSS notes that, central to risk management and mitigation is the securitization of asymmetric attacks with transnational reach, stating: 'we have wrestled with how to advance

American interests in a world that has changed – a world in which the international architecture of the 20th century is buckling under the weight of new threats' (The White House 2010: 1) The extensive discussion that is dedicated to putting forward ' [c]onstructive national steps on issues ranging from nuclear security to climate change' in the 2010 NSS, reinforces the notion that the global age has welcomed territorially unbound constructs that influence national security (The White House 2010: 27-30).

Cybersecurity is framed within the 2010 NSS as a territorially unbound sphere wherein risk must be secured in order to mitigate existential threats to US critical infrastructure and key resources (CIKR) (The White House 2010). As the 2010 NSS notes: '[c]ybersecurity threats represent one of the most serious national security, public safety and economic challenges we face as a nation…Our daily lives and public safety depend on power and electric grids, but potential adversaries could use cyber vulnerabilities to disrupt them on a massive scale' (The White House 2010: 27). Should the risks affiliated to cyberspace not be managed and mitigated by cybersecurity frameworks, the 2010 NSS (The White House: 1-8) warns that such risks pose threats to national infrastructure, diplomatic efficiency and overall economic competitiveness. Figure 1.1 illustrates the main social processes that underpin the content of the 2010 NSS.

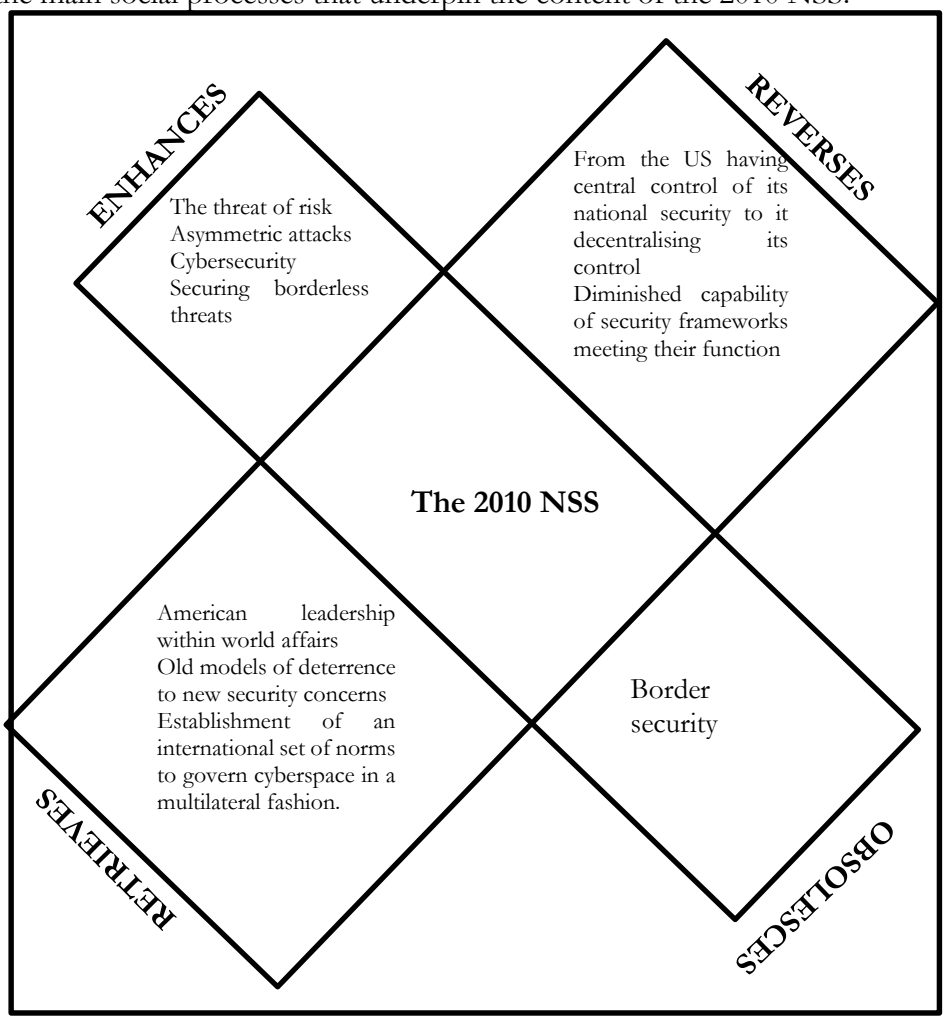


Figure 1.1 - The social processes underlying the 2010 NSS - Adapted from McLuhan's Tetrad of Media Effects (Stamps 2001)

The Social Construction of the 2010 NSS

The improved capacity of foreign nation states to challenge the national security of other nation states through asymmetric means such as cyberspace, provides further justification for national governments to propagate the prioritization of risk within securitization discourse. The gradual preoccupation of risk within US securitization discourse has led to the development of much contestation within security studies. Kessler (2010: 17-18) voices the theoretical constraints that accompany the notion of 'risk' in new security studies. Kessler (2010: 19-21) argues that conceptualizing risk in security studies leads to confused conceptualizations over threats that are not in actual fact threats, but rather natural uncertainties that do not need to be secured. Unlike Kessler (2010), Weber and Lacy (2010: 240-242) do not denounce the very real threats that vulnerabilities of the global age pose. Instead, Weber and Lacy (2010: 242) discuss the need to establish a fresh approach to designing conceptual frameworks for securitization. Without a new manner of thinking being adopted over security designs, Weber and Lacy (2010) argue that vital elements to new age securitization are being overlooked. Without denouncing any of these existing debates, an analysis of the dominant discourses from 2006-2010 opens up to an understanding of the forces that have propelled risk into action as a priority within securitization discourse.

Dominant State Rhetoric

Existential threats affiliated with cyberspace have been persistently acknowledged in US state rhetoric (2002-2010). In 2003, the United States Computer Emergency Readiness Team (US-CERT) was established by the DHS to work toward reducing cyber threats and vulnerabilities (Wagner 2012). Also in 2003, the Bush administration launched the National Strategy to Secure Cyberspace, to instill a greater sense of urgency for the securitization of cyberspace among policy makers and the public sphere (The White House 2003). Despite acknowledging the security concerns that accompany cyberspace, the securitization of cyberspace had not emerged as a priority within the NSSs up until after several cyber-attacks backed by foreign states were launched against the US.[264] In June 2007, a series of cyber-attacks, starting with the hacking of the US Secretary of Defense's unclassified email account, were being carried out on the Pentagon in attempt to access and exploit networks (NATO 2013). The gradual increase in cyber threats by foreign intruders pushed cybersecurity and the threat of risk to the forefront in national security agenda setting. In attempt to secure risk within cyberspace, dominant state rhetoric adopted a strong military stance as a functional approach toward cybersecurity, with particular focus on safeguarding the US's CIKR's and economic assets.

The militarization discourse that accompanies dominant state rhetoric on cybersecurity is evident in the emergence of US CYBERCOM in June 2009 (Wagner 2012: 18). US CYBERCOM was established in order to further the US's offensive and defensive military capabilities in cyberspace. Coupling militarization discourse and cybersecurity as such, set in motion training programmes to mobilize what are referred to as 'cyber warriors'. Such coupling indicates the use of pre-established

[264] In 2007 Estonia's parliamentary, banking, ministerial and media-linked websites were brought down by hackers allegedly supported by the Russian government. Similarly, in 2008 cyber attacks were launched against Georgia's government. Moreover, in 2009, the social networking site Twitter is said to have enabled a revolution in Iran over election unrest. Furthermore, 2009 reports indicate that the data of a multibillion-dollar fighter jet, the F-35 Joint Strike Fighter, was downloaded by hackers.

techniques of deterrence that had been designed to deter identifiable enemies and threat. This approach, however, fails to account for the borderless and ungovernable nature of cyberspace, thereby failing to secure cyberspace to the desired function that dominant state rhetoric propagates.

The push by state rhetoric for stronger functional securitization of cyberspace to manage and mitigate the threat of risk to CIKR's and economic assets is highlighted by the June 2006 National Infrastructure Protection Plan (NIPP). Designed to fulfil the requirements of the Homeland Security Presidential Directive 7 (HSPD-7), the NIPP aims to prevent, deter, neutralize, or mitigate threats to US CIKR (US Department of Homeland Security 2009a). To ensure functional success of CIKR protection, the NIPP lays out 18 supporting sector-specific plans (SSPs) to guide the activities of key regulatory agencies within an integrated structure aimed toward CIKR safeguarding, with special consideration of the dimension of cyberspace. In Section 1.5 of the NIPP, it is noted that '[t]he US economy and national security depend greatly and increasingly on the global cyber infrastructure. Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR' (US Department of Homeland Security 2009b). Extending on the central position of cybersecurity to US national security, the NIPP identifies the need for better partnerships between the private and public constituents of US society to be established, calling for the formation of an international framework to govern norms and regulations in cyberspace. Such emphasis on these aspects in a key government document reinforces the broader shift in US securitization from prioritizing physical border security to prioritizing the safeguarding of US assets with transnational reach. Figure 1.2 illustrates the dominant dimensions that underpin state rhetoric on matters of securitization prior to the 2010 NSS.

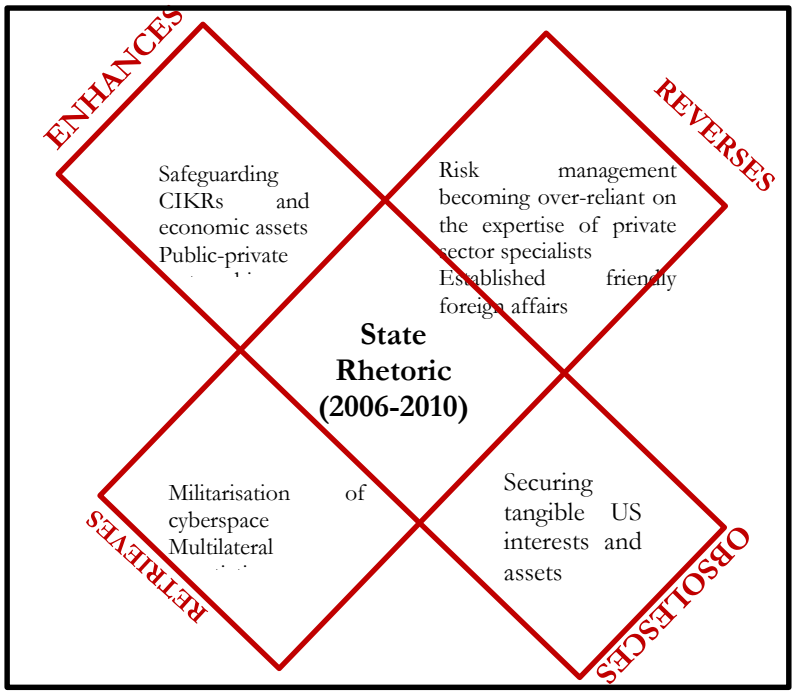


Figure 1.2 - The relative contribution of state rhetoric (2006-2010) – Adapted from McLuhan's Tetrad of Media Effects (Stamps 2001)

Although the dominant state rhetoric advocates the need for more effective national security frameworks toward securing cyberspace, by the passing of the 2010 NSS, the functional successes of national security initiatives on cyberspace fall short prior to the 2010 NSS. Williams (2010: 11) argues that such lack in success stems from there being no established lexicon in relation to cybersecurity. No established lexicon introduces drawbacks to the development of national strategic direction and goal setting. Gray (2013: 13-18) extends on this argument and notes that the little established agreement on lexicon and policy perspectives - as represented by the dominant state rhetoric on the securitization of cybersecurity - leads to misunderstood and subsequently exaggerated national security discourse on cybersecurity. The exaggerated national security threats affiliated with cyberspace, as propagated by state rhetoric, are reiterated in the dominant public sphere discourse.

Dominant Public Sphere Discourse

The function of cybersecurity advocated in public sphere discourse aligns with that advocated by state rhetoric. Public sphere discourse acknowledges that existential threats stem from cyberspace and thus, cybersecurity must be better developed in order to manage and mitigate the likelihood of cyber threats to national security. Notwithstanding the inclination toward the securitization of risk in cyberspace, tensions emerge between the public sphere and state rhetoric on the abolition of online liberties with the form of cybersecurity advocated by state rhetoric. The public sphere discourse posits that the rigid surveillance-based securitization advocated by state rhetoric for national cybersecurity, undermines the social rights of democratic communication on which the public sphere is built.

The gradual rise in activity by the international online network of activists and hacktivists that act under the name of *Anonymous* reinforces the public sphere denouncement of cybersecurity initiatives advanced by state rhetoric. Established in 2004, *Anonymous*'s initial purposes were to establish an online entertainment community (Kelly 2012: 1663-1665). By 2009, however, *Anonymous* had developed into an organized hacktivist community making use of cyber protest to instigate political and social statements against cyber-surveillance and cyber-censorship. In 2010, *Anonymous* launched cyber protests against the anti-online piracy rhetoric of Aiplex Software, the Recording Industry Association of America and the Motion Picture Association of America in the form of distributed denial of service attacks (DDoS). DDoS attacks involve the saturation of a network or machine with external communication to make them dysfunctional (Wagner 2012: 19). Following these attacks *Anonymous* released a press release stating that:

> Anonymous is tired of corporate interests controlling the internet and silencing the people's rights to spread information, but more importantly, the right to SHARE with one another. The RIAA and the MPAA feign to aid the artists and their cause; yet they do no such thing. In their eyes is not hope, only dollar signs (Tsotsis 2010: paragraph 2).

The cyber protests launched by *Anonymous* highlights the appeal within public sphere discourse for cybersecurity to adopt a form that will not repress the free flow of information which characterizes cyberspace as democratic. Figure 1.3 highlights the dominant dimensions that underpin the public sphere discourse prior to the 2010 NSS.

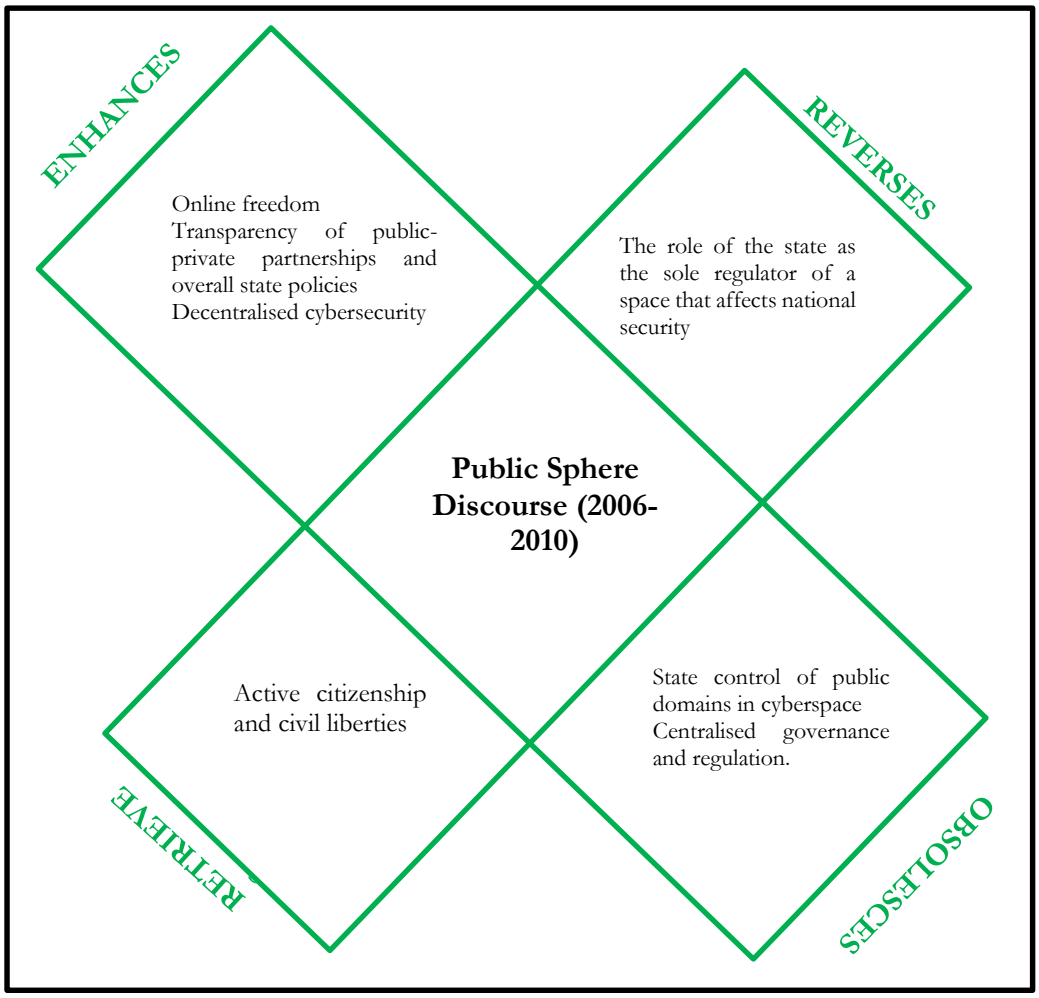


Figure 1.3 - The relative contribution of the public sphere discourse (2006-2010) – Adapted from McLuhan's Tetrad of Media Effects (Stamps 2001)

The strongly supported activism and hacktivism of *Anonymous* emerges as a direct representation of the public sphere discourse held toward cybersecurity and the securitization of risk within cyberspace. The public sphere discourse evidently aligns with state rhetoric in that it also advocates the need for US securitization to adopt the function of securing risk within cyberspace. It disapproves, however, of the form that state rhetoric advocates for cybersecurity.

Dominant Corporate Elite Interests

The cyber domain has emerged as central to the activities of corporate networks; allowing corporations ease in operations and increase business transactions vis-à-vis the elimination of time and space constraints.

The primary concerns that are advanced in corporate elite interest discourse are corporate espionage and disruptions to business operations through cyber-attacks. The TJX Financial Data Thefts that took place periodically between July 2005 and January 2006, illustrates why cybersecurity is framed as a top priority for risk securitization within corporate elite interests (Armerding 2012). Through exploiting vulnerabilities within the systems of the corporate network of TJX Companies Inc. and stole the data of 94 million credit card records (Armerding 2012). Similarly, in 2009, an employee of Valspar Corporation downloaded confidential proprietary paint

formulas worth $20 million, to provide to a Chinese corporation (Office of the National Counterintelligence 2011: 47). Such economic espionage via cyber-attacks results in costs to major corporations, in the form of unique intellectual property to outlays for remediation. Symantec, an American security software company, places the cost of intellectual property theft at $250 billion a year to the US economy. Meanwhile, McAfee provides an estimate encompassing global remediation costs to total a staggering $1 trillion per annum. Moreover, the Valspar Corporation case highlights the need for risk securitization in cyberspace for national security purposes. Cyber espionage is not merely carried out within the physical borders of the US where such cyber-attacks can be legally rectified. Instead, cyberspace has emerged central to the interactions between nation states, therefore holding the potential of emerging as an economic battleground between nation states competing in power projection. Operation Aurora, reported by Google in January 2010, involved the exfiltration of intellectual property rights by Chinese hackers from Google China (Branigan 2010). Operation Aurora, is a key illustration of this, thereby posing a threat to national security.

Provided that most of US critical infrastructure is owned and regulated by the private sector, corporate elite interests hold a strong influence on the form that US cybersecurity policy initiatives adopt (Michael Losavio 2013: 19). The corporate elite interest discourse argues that, should the US private sector not be safeguarded from risks of foreign cyber-attacks, the likelihood of national security threats in the form of economic costs and damage to CIKR's increases. In order to better secure the accelerated exploitation of vulnerabilities in cyberspace, and manage the risks to the US private sector, strong partnerships have emerged between the state and the private sector as a means of granting the private sector with greater regulatory rights in cybersecurity initiatives. The Federal Information Security Management Act (FISMA), and its numerous reforms, illustrates the movement within cybersecurity to improve public-private partnerships; the very kind of partnerships that the 2010 NSS emphasizes. FISMA has established standards and regulations that must be adhered to by the cyber activities of state agencies and private corporations under the auspices of the Office of Management and Budget (OMB) (Michael Losavio 2013). The FISMA standards and regulations force the establishment of minimum systems security protocols, annual reports of cyber threat incidents, government procurement of business regulations and transparency of corporate business activity. Figure 1.4 illustrates the dominant dimensions that underpin the corporate elite interest discourse (2006-2010).

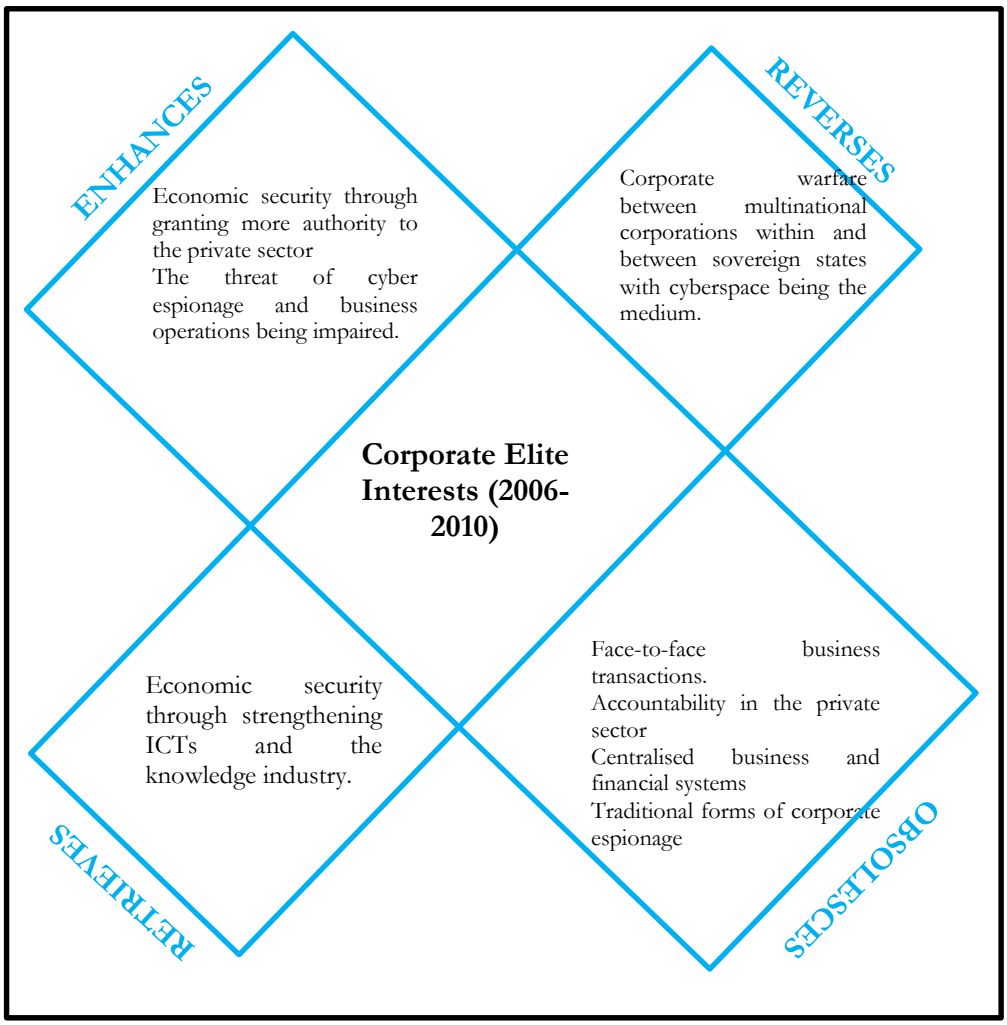


Figure 1.4 - The relative contribution of corporate elite interests (2006-2010) – Adapted from McLuhan's Tetrad of Media Effects (Stamps 2001)

The central authority that corporate elite interests have over cyberspace places the dominant discourse at the forefront of deciding how risk ought to be managed and mitigated within cybersecurity frameworks. The corporate elite interest discourse, therefore, emerges as a predominant contributor to the emergence of the 2010 NSS securitization framework on risk within cyberspace.

The Outcome of Dominant Discourses on the 2010 NSS

Having deliberated upon the respective dominant discourses of on cybersecurity, it is seen that across these variables, consensus is reached on the necessity of cybersecurity to ensure the management and mitigation of existential risks posed by the exploitation of cyberspace vulnerabilities to US national security. Much contestation, however, surfaces between the dominant discourses over how cybersecurity should be ensured.

The dominant discourses held by state rhetoric and the public sphere discourse on the securitization of risk within cyberspace, are respectively fueled by the notion that existential risk may materialize at any point in time. Using the element of uncertainty that accompanies ungovernable constructs and notions of risk, state rhetoric forecasted potential scenarios of 'cyber

Pearl Harbor's', thereby, providing a stronger sense of legitimacy to national security policies advanced by state rhetoric on cybersecurity. In October, 2012, Defense Secretary Leon Panetta warned that the US was facing the possibility of a 'cyber Pearl Harbor' in light of accelerated foreign attacks on US cyber networks (Shanker 2012). Drawing on the historical analogy of Pearl Harbor, associates an identifiable national memory to what are framed as probable, but not certain threats emanating from cyberspace.

Notwithstanding the consensus on the need to secure risks within cyberspace to ensure national security, between state rhetoric and public sphere discourse, these two variables enter into tense debate over the form that cybersecurity ought to take so that privacy and civil liberties are ensured alongside the securitization of existential threats within cyberspace. The contention that emerges between these two variables speaks to the incongruences that exist within the legal, political and social spheres on intangible constructs such as cybersecurity. Such incongruences further impair advances toward bridging the form and function of securing risk within cyberspace. This is further highlighted by the emergence of cyberspace as an economic and military battlefield between nation-states. Due to the cross-border interactions that cyberspace facilitates, the issue of jurisdiction has become a major obstacle to cybersecurity within national security frameworks. Should a cyber-attack be conducted on the US by an individual in a different nation state, the lack of a comprehensive legal framework that can be used to penalize such attacks has emerged highly problematic within discussions of cyber threats to national security. The lack of jurisdictional frameworks that enable proportional penalties to cyber threats on national security has pushed forward the discourse that an international regulatory framework needs to be developed in order to ensure that the lack of appropriate securitization of risk within cyberspace does not lead to the outbreak of cyberwar between nation states.

The discourse of existential crises that is mirrored across the dominant discourses, is not impossible, but it is improbable. Despite the technically low probability of existential cyber-attacks, the permeation of the notion of such attacks across the discourses is enough to propel forward the socially constructed idea that the securitization of risk within cyberspace is necessary to ensure US national security. Basing the form and function of securitization discourse on predicted likelihoods of cyber-attacks instead of on certain identifiable threats, has sparked criticism from scholars in new age security studies, claiming that basing securitization on intangible threats impairs adequate policy formation. Farwell (2012: 13) posits that focusing securitization on risk leads to competing policy perspectives on how best to manage territorially unbound constructs such as cybersecurity between government bodies. Dunlap extends from the argument that the securitization of unbound constructs generates competing policy perspectives, and raises the consequent issue of proportionality (Dunlap 2008: 718-720). Dunlap claims that proper policy implementation for securing risks within cyberspace is prevented by such differing policy perspectives. Farwell (2012) and Dunlap's (2008) respective studies speak to the dominant discourses at play within US cybersecurity and the problem the incongruences between dominant discourses pose to effective national security formulation.

The dynamics between state rhetoric, public sphere discourse and elite interests indicate that the securitization of risk within cyberspace is predominantly informed by a security-economic nexus. The dominant state rhetoric and elite interest discourses both advocate that the form and function

of securing risk within cyberspace must place precedence on securing US CIKRs and US economic assets, most notably intellectual property rights.

Furthermore, when contrasting the advocated securitization in the 2010 NSS with those of pre-emptive security and retaliatory security before it, a noteworthy shift in international US engagement is highlighted. Unlike the 2002 and 2006 NSS's, where US intervention was justified by the threat of rogue states discourse, the 2010 NSS justifies international US engagement and foreign intervention on the need to secure 'at-risk- states' (The White House 2010). This shift in discourse for justifying acts of US foreign intervention speaks to a broader shift in the priorities that inform US securitization in the 21st century. Furthermore, it reinforces the shift in US securitization from prioritizing physical security to prioritizing the securitization of risk-based threats to US interests and assets.

The security-economic nexus that emerges from the dominant discourses in state rhetoric and elite interests propelling forward the shift from a pre-emptive stance toward the securitization of risk, leads to the framing of ungovernable spaces as possible existential threats rather than actual identified existential threats. Such risk-based discourse, therefore, is reliant on the interaction between state rhetoric, public sphere discourse and elite interests to guarantee legitimacy for introducing new regulatory frameworks in the name of national security.

Conclusion

Using cyberspace as an illustration of a territorially unbound construct with direct influence to national security, the emergence of risk securitization as a national security priority in the 2010 NSS has been identified.

The urgency for securing cyberspace across the constituents of state rhetoric, public sphere discourse and elite interests following 2006 saw a greater integration of form and function in cybersecurity initiatives between the private and public sectors. The strong presence of state rhetoric and elite interest discourse within the realm of cybersecurity, however, illustrates that public sphere discourse does not exist autonomously from state and economic power, and is therefore the least relative contribution to the form and function of risk securitization in cybersecurity frameworks. Figure 1.5 captures the relative contribution of state rhetoric, the public sphere and corporate elite interests to the 2010 NSS content.

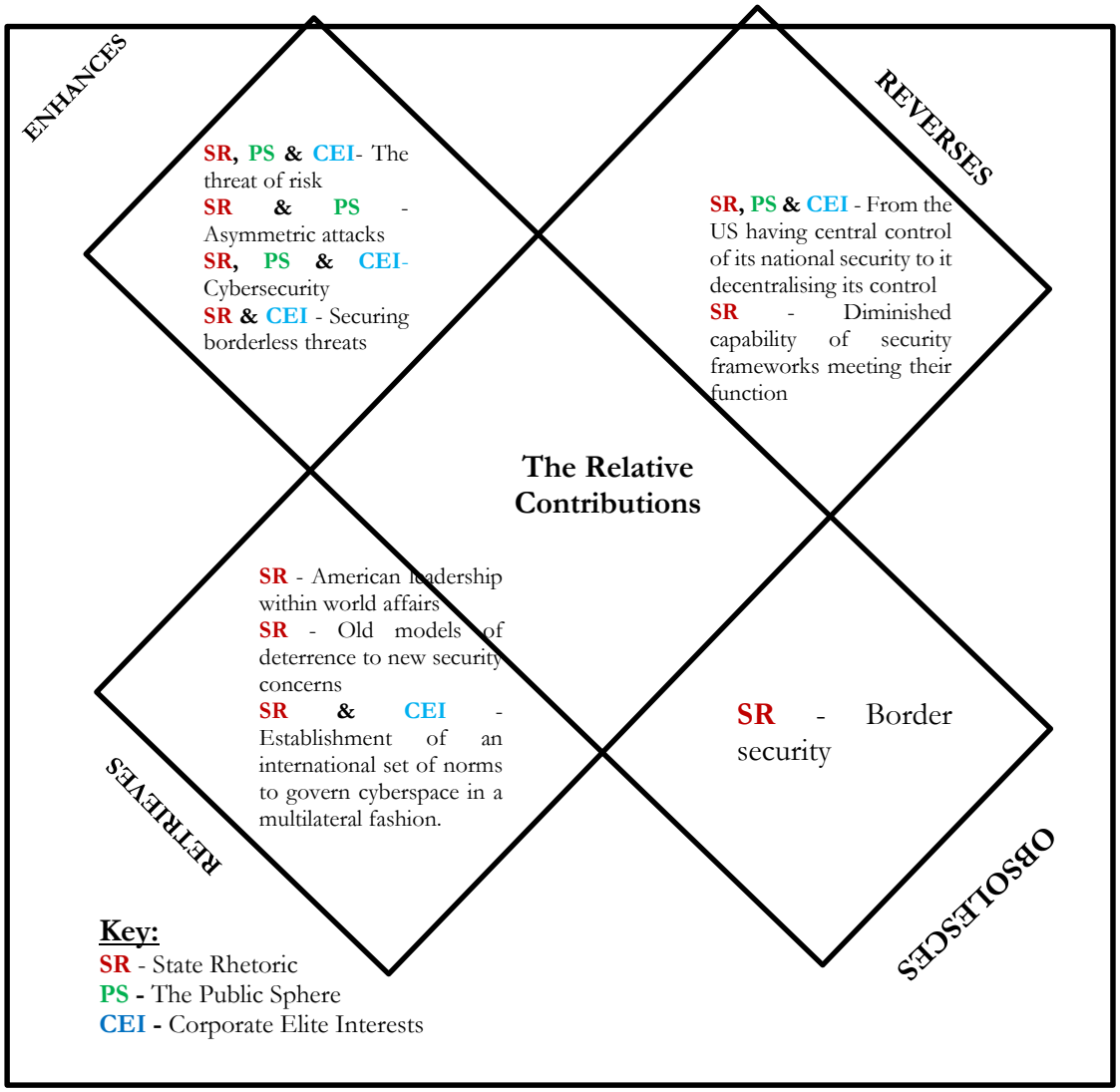


Figure 1.5 - The relative contribution of the dominant discourses to the 2010 NSS - Adapted from McLuhan's Tetrad of Media Effects (Stamps 2001)

The prioritization of risk securitization within US cybersecurity frameworks emerges as a prime example to the shifting nature of US securitization in the 21st century. The dominant state rhetoric, public sphere discourse and corporate elite interests that have contributed to the emergence of cybersecurity as a priority in US securitization discourse highlights the gradual movement and dynamics behind the securitization of risk and protection of intangible US assets, rather than tangible US borders.

RECOMMENDATIONS FOR FUTURE ANALYSIS

The evolution of US securitization in the 21st Century has shifted from placing precedence on reactionary securitization of identifiable threats, toward placing precedence on securing the potential threats. The notion that national security approaches are shaped by, and subsequently inform the dominant discourses of social constituents such as state rhetoric, public sphere discourse and corporate elite interests, has been maintained from having deliberated upon evolutions within US securitization. An examination of the dominant discourses and their respective contribution to the emergence of guiding NSSs, sustains the notion that certain

discourses have a greater contribution over others on the emergence of dominant securitization discourse.

The shift in securitization from the 2006 NSS to the 2010 NSS illustrates a broader shift in securitization, from securing US physicality from identifiable threats both within and outside national borders, to prioritizing the security of US interests and assets from intangible and territorially unbound threats. This broader shift in securitization is informed by social forces such as state rhetoric, the public sphere and corporate elite interests and propelled into being. The interaction between the three dominant discourses of state rhetoric, elite interests and public sphere discourse makes it clear that state rhetoric holds the most influential position in determining the form and function of securitization strategy adopted. Public sphere discourse and corporate elite interests act to either support or challenge the form and function of securitization strategy advanced by state rhetoric. Understanding the relationship between the social forces that inform the emergence of an NSS is essential to designing effective securitization strategies that encompass all the elements needed to manage the dominant threat matrixes of a particular historical context.

Having examined the social construction of US securitization strategy as a national artefact seemingly informed by local interests but framed within international uncertainty, it becomes clear that the function and form of securitization strategies have been, and continue to be incongruent. Such incongruences emerge as problematic for managing national security threats, in the process of both policy formulation and policy implementation. The gradual shift within US securitization toward risk securitization enhances existing concerns with regard to the successful management of national security threats. The prioritization of risk as a threat within national security approaches makes any issue open to securitization. Any issue framed as 'risk' and politicized into securitization within national security approaches, enhances the incongruences between the form and function of securitization. In order to minimize problems that arise from incongruences between the form and function of securitization discourse, a better understanding needs to be developed on why and how securitization discourses enter into action and evolve alongside the changing contours of social constituents of a given civilization. This article offers a preliminary approach for developing a more holistic understanding of how and why securitization discourses come into existence. It does not, however, deliberate enough upon the evolution of risk securitization into its current existence.

This article utilizes cybersecurity as an illustration of the precedence of risk securitization within US national security approaches. The securitization of risk within US national security approaches, however, has taken precedence across numerous dimensions of US civilization; dimensions which fall outside the scope of what will be elaborated on here. Further research needs to be directed toward understanding the evolution of securitization discourse so that such discourse can either be altered to prioritize more governable constructs, unlike risk within national security approaches, or to design new policy frameworks that minimize incongruences between the form and function of securitization.

In addition to recommending that further research be conducted on the social construction of dominant securitization discourses, so that better informed security policies can be design and implemented, it is also recommended that the subject of securitization is better defined. From the analysis conducted on one focal point to the evolution of US securitization strategy, it can be seen

that the incongruences between the form and function of a particular securitization discourse are enhanced if the subject to be secured is not simple to identify. In effect, subjects of securitization such as 'risk' need to either be altered into more specific and tangible subjects, or a collective understanding must be met across all social constituent discourses over what risks consists of. The use of constructs that have no established contextual definition to the security context prevents the appropriate establishment of the social order needed to maintain that construct within a dominant discourse of securitization.

Moreover, the numerous incongruences that emerge between the form and function of securitization within the phase of securitization (2006-2010) analyzed herein, indicates that securitization discourse is not necessarily effective in meeting its function of securing an identified subject. Drawing on the basic assumptions made by Balzacq (2005), I advocate that the following assumptions must be reflected within securitization discourse to ensure that it is effective:

a. The securitization must be audience-centered

b. It must be context-dependent

c. It must be power-laden

Through ensuring that the aforementioned assumptions are reflected within a securitization discourse, the incongruences between the function and form of securitization are less, thus, allowing for better alignment between security policy design and implementation.

Lastly, when regarding the form of securitization advanced across the respective discourses within the securitization of risk, it is seen that traditional security methods, such as deterrence, are being used within new and unfamiliar securitization frameworks such as cybersecurity. Traditional security methods, however, do not adequately manage the threats that accompany territorially unbound constructs such as cyberspace. In effect, new security methods must be developed in response to the new and unfamiliar constructs that have emerged as dominant within US securitization discourse.

References

Armerding, T. (2012). The 15 worst data security breaches of the 21st Century. *Security practitioners weigh in on the 15 worst data security breaches in recent memory*. http://www.csoonline.com/article/700263/the-15-worst-data-security-breaches-of-the- 21st-century

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations, 11*(2), 171-203.

Bennett, C. J., & Howlett, M. (1992). The lessons of learning: Reconciling theories of policy learning and policy change. *Policy Sciences, 25*, 275-294.

Branigan, T. (2010, 13 January). Google to end censorship in China over cyber attacks. *The Guardian* Retrieved from http://www.theguardian.com/technology/2010/jan/12/google-china-ends-censorship

Bumiller, E., & Shanker, T. (2012, 11 October, 2012). Panetta Warns of Dire Threat of Cyberattack on U.S. . *The New York Times*.

Counterintelligence, E. O. o. t. N. (2011). *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*. Washington.

Dunlap, C. (2008). Toward a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors. *Nebraska Law Review, 87*(3), 712-724.

Farwell, J. P. (2012). Industry's Vital Role in National Cyber Security. *Strategic Studies Quarterly*, 10-42.

Gray, C. S. (2013). Making Strategic Sense of Cyber Power: Why the Sky is Not Falling (pp. 83). Pennsylvania: Strategic Studies Institute.

Holborn, M. H. M. (2004). *Sociology. Themes and Perspectives*. Hammersmith, London: HarperCollins.

House, T. W. (2010). *The National Security Strategy* Washington DC: The White House.

House, T. W. (2006). *The National Security Strategy of the United States of America.*

Kelly, B. B. (2012). Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" can and Should Influence Cybersecurity Reform. *Boston University Law Review, 92*, 49.

Kessler, O. (2010). Risk. In P. J. Burgess (Ed.), *The Routledge Handbook of New Security Studies* (pp. 10). New York: Routledge.

Kenis, P., & Schneider, V. (1991). Policy Networks and Policy Analysis: Scrutinising a New Analytical Toolbox. In B. M. a. R. Mayntz (Ed.), *Policy Networks. Empirical Evidence and Theoretical Considerations* (pp. 38). Frankfurt: CO: Campus Westview.

Klippstein, L. C. D. M. (2003). Homeland Security: The Department of Defense, The Department of Homeland Security, and Critical Vulnerabilities. In W. Murray (Ed.), *National Security Challenges for the 21st Century* Pennsylvania: Strategic Studies Institute.

Liotta, P. H. (2005). Through the Looking Glass: Creeping Vulnerabilities and the Reordering of Security *Security Dialogue, 36*(1), 149-172.

Losavio, M., Shutt, J. E., & Keeling, D. W. (2013). Changing the Game: Social and Justice Models for Enhancing Cyber Security In L. H. J. J. Tarek Saadawi, Vincent Boudreau (Ed.), Cyber Instrastructure Protection (Vol. II). Pennsylvania Strategic Studies Institute.

NATO (Producer). (2013, 8 October). The history of cyber attacks - a timeline *NATO Review Magazine*. Retrieved from http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

Security, U. D. o. H. (2009). *National Infrastructure Protection Plan: Partnering to enhance protection and resiliency* Washington DC: The White House.

Security, U. D. o. H. (2003). *The National Strategy to Secure Cyberspace* Washington DC: The White House.

Snow, N., & Taylor, P. M. (2006). The Revival of the Propaganda State: US Propaganda at Home and Abroad since 9/11. *International Communication Gazette, 68*(5-6), 389-407.

Stamps, J. (2001). *Unthinking Modernity: Innis, McLuhan, and the Frankfurt School* Quebec City: McGill University Press.

Tsotsis, A. (2010). RIAA Goes Offline, Joins MPAA As Latest Victim of Successful DDoS Attacks http://techcrunch.com/2010/09/19/riaa-attack/

Waever, O. (1995). Securitization-Desecuritization In R. Lipschutz (Ed.), *On Security* New York: Columbia University Press.

Wagner, A. R. (2012). Cybersecurity: from experiment to infrastructure. *Defence Dossier,* (4), 29. http://www.afpc.org/files/august2012.pdf

Weber, C., & Lacy, M. (2010). Designing Security In J. P. Burgess (Ed.), *The Routledge Handbook of New Security Studies* New York: Routledge.

Williams, P. A. H. (2010). *Information Warfare: Time for a redefinition.* Paper presented at the Australian Information Warfare and Security Conference Perth.