UNIVERSITY OF GOTHENBURG

Securitizing the Virtuality of the Real

A Gramscian Analysis of the Securitization of U.S. Cyberspace Governance

Dennis Halvordsson

Bachelor Thesis in International Relations

University of Gothenburg

School of Global Studies

Autumn 2012

Supervisor: Jan Bachmann

Abstract

This thesis analyzes the contemporary conformations of governance in the U.S. discourse on cyberspace through a Gramscian theory of International Relations. The thesis primarily focuses upon the question of governance through the analysis of a potentially ongoing securitization process in the realm of cyberspace governance. This process is located by a critical discourse analysis on the Cyberspace Policy Review, a U.S. governmental document that summarizes all of the near- and mid-term policy issues for security in cyberspace. As such, a qualitative research design was utilized in the study. The prevalence of securitization is further explained within the framework of hegemony. Hegemony, as a distinct conformation of governance, argued by this thesis, seems to be especially consanguineous to the phenomenon of securitization. There is a tendency that the subjects of governance is not sought for consent at face value, rather, a securitization process seem to be the very condition for them to enter into the hegemonic order.

Key words: Gramsci, cyberspace, governance, securitization, hegemony, critical realism, international relations, United States, security studies, critical discourse analysis.

Acknowledgements

I first of all wish to thank my supervisor Jan Bachmann for his engagement and valuable theoretical and methodological guidance throughout my work on this thesis. I would also like to thank Roland Heickerö at FOI for some valuable advices. Further I would like to thank my close friends Otto Widmark, Hanna Ricksten, David Westerberg, Per-Erik Nyström, Lovisa Möller, Jimmy Emanuelsson, and Hannes Hognert for sharing their thoughts on the thesis.

For my mother

Table of Contents

List of Abbreviations

CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
CISO	Chief Information Security Officer
CNCI	The Comprehensive National Cybersecurity Initiative
DARPA	Defense Advanced Research Projects Agency
DNI	Director of National Intelligence
EOP	Executive Office of the President of the United States
GLP	Government liability protection
FAA	Federal Aviation Administration
HSC	Homeland Security Council
ISPAB	Information Security and Privacy Advisory Board
ISR	Information sharing regime
ITU	International Telecommunications Union
JIACTF	Joint Interagency Cyber Task Force
NSB	National Science Board
NEC	National Emergency Council
NIAC	National Infrastructure Advisory Council
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSF	National Science Foundation
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
OMB	Office of Management and Budget
OSTP	Office of Science and Technology Policy
PCLOB	Privacy and Civil Liberties Oversight Boar

1. Introduction

1.1. The 'Passive Revolution' of American Cyberspace

The principal inquiry of problem in this thesis will evolve around the apparent problems for states to govern or establish sovereignty over cyberspace, and the possibility of a securitization process accompanying these activities. The term 'cyber sovereignty' (which is not yet very extensively analyzed) indicates that we are talking about sovereignty in the classical sense of state sovereignty (Bull 1977), although in a different (contingent upon ontological understanding) environment or realm; the *cyberspace*. Drawing upon the works of major scholars on *sovereignty*, the wider definition of such term entails the sovereign rule of a political entity over a certain population, on a certain geographical territory (Bull 1977; Biersteker & Weber 1996: Krasner 1999; Philpott 2001). This capability or praxis hinges on the legitimacy of both internal and external actors (Krasner 1999: 4ff). It needs the legitimacy from the governed population and from the surrounding sovereigns (ibid.; Hannum 1996: 15). In great simplification, adding with recent global communitarian aspects of sovereignty as a 'responsibility' (Etzioni 2006; Glanville 2011), this is the main elements of the international system since the peace of Westphalia in the year of 1648.[1]

Following the digital revolution of the late 1990s and 2000s the activities of states have by now moved into the realm called 'cyberspace'. It is alleged that the first "cyber war" was fought in the year of 2007, when Estonia was attacked by anonymous groups situated within the Russian Federation (Heickerö 2012: 15). These developments of militarization in cyberspace have also led states into a necessity of defining their territory in cyberspace (Nagorski 2010; McEvoy Manjikian 2011: 383; Heickerö 2012: 196). In order to know what to protect, you need to define it (Campbell 1998: 170). This is easier said than done. If for example, the nation-state Sweden decides to lay sovereign claim over all servers affiliated to the state-controlled domain .se, it is probably the case that the real geographical locations of these servers are spread out all across other territories around the globe (Heickerö 2012: 190). Consequently, sovereignty is difficult to apply, and norms of behavior for warfare are still only vaguely defined (ibid.: 196; Joyner & Lotrionte 2001; Hughes 2010). This also means that the question of security is a rather elusive subject in the realm of cyberspace.

[1] The concept of 'sovereignty' is also further modified and adapted within different disciplines, such as 'mobile sovereignties' (Appadurai 2006), 'graduated sovereignty' (Ong 2000), 'viral sovereignty' (Mullis 2009), to name a few. But these are not concerned within the frame of the discipline of this thesis.

Therefore, to try to capture this elusiveness and explain some of the main features of cyberspace governance, one might need to pay attention to the possibility of an ongoing securitization process. This process can, tentatively, be found through discourse analysis of the *Cyberspace Policy Review* created on the initiative of the contemporary U.S. administration. The document was assessed during 60 days and collects the interests of state, market and civil society considering the governance of cyberspace. The document also underscores some indications for the formulation of a foreign policy of cyberspace.

The reason for analyzing the U.S. cyberspace policy stems from the central role this actor performs within cyberspace governance. As many scholars of International Relations have concluded, the development of cyberspace is to a large extent of American origin (McEvoy Manjikian 2010) and is also a critical feature of the, by now post-Fordist, global capitalist economy that grew out of American capitalist modes of production. But cyberspace is not ruled by any iron fist of state. It is more appropriate to designate it as a kind of hegemonic order. The works of Antonio Gramsci (2010) and the concept of hegemony, is hitherto relevant. It can visualize the structure of contemporary cyberspace in suitable abstraction. As having sprung out of the dialectics of American social forces, cyberspace (itself) is the *passive revolution* par excellence (See section 2.2.). It effectively establishes an order of global – provided the access of technology exists – magnitude that impinges upon the periphery a dynamic which rapidly enforces another mode of social interaction (See McEvoy Manjikian: 385), and maybe even creates the predicament for social revolutions. Tantalizing is the thought, to expound cyberspace as having the appearance of an *Empire* in Michael Hardt and Antonio Negri´s sense of the word. One which does not concern boundaries or territory. Presumptively, it is rather an *Empire* constituted by respatialization, and a constant tendency to a *hegemony of diversity* as the contemporary dynamics seem to indicate (Cox 2001; Clark 2009, 2011), although in relative decline (Ned Lebow & Kelly 2001).

In Simon Bromley's words "power resides ultimately in the multitude" (2003: i). The complexity and interconnectedness of cyberspace has so far effectively resisted any sovereign boundaries. The question therefore remains as to what kind of instruments of governance we can expect to emerge. The U.S. establishment has clearly identified a number of threats inherent to cyberspace itself. Consequently, having made them called upon the specter of security to defend the Nation (Knake 2010; Segal 2011). A process of cyberspace securitization might therefore be imminent. This establishes the subject basis for the scientific inquiry of this thesis.

1.2. Disposition of Thesis

The disposition of this thesis comprises of six chapters. The introductory chapter outlines problem and inquiry of research (1.3.), purpose and relevance of research (1.4. & 1.5.), and delimitation of scope (1.6.). I will then proceed by presenting the major previous research on the subject (2.1.), and how this thesis desires to tap into these works. This is followed by an account on the theoretical premises of this thesis (2.2.), and the theory of securitization applied (2.3.). The third chapter outlines the qualitative method of critical discourse analysis (3.1.-3.3.) and the procedure of data analysis (3.4.), as well as the weaknesses of this endeavor (3.5.). The analysis and results chapter is split into four sections. The analysis of securitization is conducted within [4.1.], [4.3.], and [4.4.], while the analysis of governance is comprised within [4.2.]. This might be confusing, but necessity had it that I outlined the context (4.1.) before embarking on the analysis of governance (4.2.). The concluding chapter (5.) draws upon conclusions from all of the four analysis sections and is followed by discussion (6.).

1.3. Research Problem & Inquiry

It is a legitimate speculation that the complexities of cyber governance described above may be once another menace for state sovereignty owing to the well-known process of globalization (Keohane 2000; Acharya 2007; Castells 2007; Choucri & Goldsmith 2010). In addition, it is an ambition of this study to make some marginal contribution to the debate on the contemporary nature of global governance. The study will approach this process as a kind of *securitization*. Two fundamental elements indicate such a process. The issue "should be a focus of public attention or debate."(Balzacq 2011), and "the issue is target for activities of legal or political actions." (ibid.) In light of the so called *Cyber Policy Review* issued by the contemporary U.S. administration; both of these criteria are evidently met. Central to the task and scientific problem of this thesis is therefore to outline the formula of cyberspace governance by the contemporary U.S. administration in order to find out whether a process of securitization accompanies the quest for governing cyberspace. Since I think it can be reasonably argued, that the behavior of the United States as a global hegemon (Saull 2012) is prescriptive to the behavior of other states, the primal foci of this thesis will be confined to the analysis of the securitizing discourse on cyberspace enacted by this actor. Subsequently, the scientific inquires reads as follows:

1) How is 'governance' represented in U.S. cyberspace policy?

2) Is it possible to identify a process of securitization within U.S. cyberspace policy?

1.4. Purpose of Research

Following these inquires; the purpose of this study is desirably to illuminate processes of cyberspace securitization accompanying ambitions of governance in order to *raise awareness* about possible 'security issues' related to these activities. This is the main explanatory value of this paper. Since this is also a critical study, it hence hinges on an understanding of the concept of *security* as inevitably a normative one (Campbell 1998; Buzan & Hansen 2009: 10ff). This thesis will take aim on questions of possible power relations connected to a securitization process within cyberspace and what these dynamics means for contemporary theories of International Relations. In sum, the purpose is therefore threefold: to shed light on spheres of governance, to sensitize a discourse of security concerned with relations of power and hegemony, and to utilize critical realist theories and methods of social science (See section 3.2-3.3.). As such, this thesis holds ambitions of both explanatory and theory developing aspects.

1.5. Relevance of Research

The scientific relevance of this study is by large the pioneering aspect of investigating a relatively new field of Security Studies. It is presumed that the introduction of the domain of cyberspace fundamentally alters the Westphalian logics of security (Acharya 2007; Choucri & Goldsmith 2010; Hughes 2010). Therefore, it can be argued that further elaboration upon this matter is to great benefit for both the scientific community, and the society at large. Primarily, as some scholars in the field of cyber warfare have emphasized, "there is no international consensus on the application of the 'law of armed conflict to cyber-warfare,'" (Hughes 2010: 531; Bajaj 2010; Heickerö 2012: 189). Since the International Community would like to establish such norms, this thesis might hopefully be of some marginal relevance as a contribution to this global discussion (See section 2.1). Secondly, since the introduction of state activity in cyberspace can be presumed to challenge conventional theories within IR this study may introduce some novel but marginal developments within the theoretical debates on the status of U.S. hegemony and its relation to the social phenomenon of securitization (See section 2.2.). Thirdly, this study will take point of departure from a critical realist perspective of social science (See Bhaskar 2008; Sayer 2000, 2010). Hence, it will try to reverse the "long-standing dogma of privileging epistemology over ontology." (Patomäki & Wight 2000: 215). The relevance of this endeavor is to my view productive for the process of social science at large (See section 3.2.-3.3.). To sum up, its relevance is both theoretical and empirical, although for the most part theoretical.

1.6. Delimitations of Scope

The inquiry of research of this thesis motivates the study of policy at the highest levels of government. As is stated above (section 1.1.), the central delimitation of this study will extend within the security policies formulated by the United States. The reason is that it is presumed that this actor, in virtue of its hegemonic position, might have a large impact on the formulation of policies by other nation-states (Saull 2012). The horizon of time for the elaboration of this thesis offers little space for a diachronic analysis concerned with the development of cyberspace policy from the outset of the digital revolution (See Castells 2001; Halpin, Trevorrow, Webb & Wright 2006 for a historical oversight). Instead, a synchronic analysis with some aspects of prevision seems to be of greater relevance.

It would further be interesting to study the different approaches to cyber governance developed within the major multilateral institutions concerned with this issue, such as the International Telecommunications Union (ITU), the International Organization of Standardization (ISO) and the United Nations. However, since these institutions consist of member-states, such an approach would necessarily be curious about the perspectives of nation-states underlying the commitments of these institutions. Therefore, the dynamics within these institutions might initially be better captured by the study of discourse within a single nation-state and its role of participation in this process.

Moreover, this thesis will exclusively focus on security and models of governance proposed by the Cyberspace Policy Review (CPR). This entails questions of control, sovereignty, use of force, and the particular interests underlying the assessment of the review. By analysis of these aspects, this thesis has the ambition to disentangle the role of state, market and civil society in this process.

An additional delimitation of this thesis is an exclusive focus on the text of the CPR, guided by theoretical premises. This is foremost motivated by the constraints on extent due to choice of method. Critical discourse analysis (See section 3.5.) offers plenty of tools for conducting a detailed and thorough analysis, but also limits the capacity to analyze large amounts of texts. Therefore, the numerous reports and documents comprised in the bibliography of the CPR will only be analyzed in terms of the identity of the actor of their origin, and will not be included in the discourse analysis *per se* (See Annex 1). This delineation will provide this thesis with a profound depth, while also narrowing the scope to a central concern on the perspective of government.

2. Theory & Discourse

2.1. Previous Research – The Virtuality of the Real

The first question to pose when studying the phenomenon of cyberspace must necessarily be an ontological one. Philosophers of various kinds have posed this question, and most of them hold the interpretative conclusion (pardon me for this simplification, philosophers) that it *is not* by its nature very different to the 'conventional world' (Žižek 1996; Koepsell 2000; Michelfelder 2000; Lessig 2002; Spinello 2002; Higham 2005; Young & Whitty 2011). The interpretation I hold most dear is that of Slavoj Žižek, which on basis of the Lacanian triad of the real, imaginary and symbolic convincingly point out that cyberspace is not a *virtual reality*, but the opposite: the *virtuality of the real* (1996). Our phenomenological interaction with it is similar. Just as in nature, 'code is law'. In this case, humans construct the code (Lessig 2006). But the code we construct is necessarily contingent on the 'real' code.

According to IR-scholar Mary McEvoy Manjikian, the major normative standpoints in the discourse on cyberspace could be divided between two (actually it's always three) inconsistent standpoints (2010): the *liberals* and the *realists*, vividly reflecting the American two-party system. But, the liberal standpoint is for some 'incomprehensible reason', also, split into two: 'utopian' and 'pragmatist' (ibid.). The first one is arguing in favor of continuous unregulated activity for a cyberspace similar to a man-made common, it is referred to as the "utopian" stance (ibid.: 384). I argue that 'utopian' is a misleading term, it should rather be denoted the *communist* standpoint. Simply because the fundamental issue at hand is that everything in cyberspace should be shared freely to promote the creativity of voluntarism (See Castells 2001). Therefore, it is rather 'communist' than 'utopian'. By locating this standpoint as one repressed side of a liberal view ('utopian' or 'pragmatist'), McEvoy Manjikian also neglects the 'political theology' intrinsic to the *hypostasis* of Western capitalist structure.

They are always three. Order, Freedom and Justice (See Abrahamsson 2008: 241).

Nonetheless, the second stance on the other hand argues for semi-regulation and a relative abolishment of anonymity, following a liberal interpretation of cyberspace as a place fit for commercialization and commodification (McEvoy Manjikian 2010: 385; Bajaj 2010**;** Cornish et al 2009). This might be called the *liberal* standpoint (not 'pragmatist' liberal).

Thirdly, a substantial proportion of voices also argues that cyberspace is yet another arena for threats and danger, and hence should be subjected to sovereign control (McEvoy Manjikian

2010: 389; Choucri & Goldsmith 2012; Hughes 2010). This is called the *realist* standpoint. McEvoy Manjikian also developed a scheme for differentiating between these views by analyzing their view of ‘territory’, ‘power’, ‘identity’, ‘credibility’, ‘information’, ‘regulation’, and ‘growth’ (ibid.: 387ff). All of these proved helpful for the identification of discourse in this thesis. Moreover, these three positions also correspond to Antonio Gramsci’s notion of a *war of positions* between civil society, market, and state (Gramsci 2010).

Further, the main questions at hand within the studies conducted so far are the development of sufficient definitions of agent/structure, violence, power, and territory within the contours of cyberspace (Nye 2010; Manjikian 2010; Bajaj 2010; Choucri & Goldsmith 2012; Hughes 2010). It is presumed that cyberspace fundamentally alters many of the mainstream ideas within IR-theory. The major threats facing states is information warfare on critical systems such as energy grids, telecommunications, and financial facilities that could cause severe disruption in vital social services (Joyner & Lotrionte 2001). And, there are no rules for right to ‘self-defense’ or qualification of ‘armed attack’ in cyberspace, as it does regarding ‘kinetic’ use of force (ibid.). ‘Cybersecurity’ therefore comprise of two dimensions: risk *to* cyberspace and risk *through* cyberspace (Deibert & Rohozinsky 2010). Moreover, the most fundamental feature when it comes to the concept of power within cyberspace is the shift in asymmetries. Small actors enjoy an advantage in terms of vulnerability since the price of entry is low, at the same time as the possibility for inflicting damage is great (Nye 2010). It is argued that the largest powers will not be able to dominate this realm as easily as they, for example, masters’ the air and sea. And therefore, cyberspace furthers the diffusion of power (ibid.). Following my theoretical premise, I agree to the plausibility of this conclusion in so far as a one/two/three-dimensional concept of power is concerned (See Dahl 1961; Bachrach & Baratz 1962; Lukes 1974), but not beyond. If a specific mode of production and social interaction in itself is facilitated by the mere structure of cyberspace, then the hegemonic interest of the social force behind it impinges upon other actors by their sheer participation in it. Just consider the potential factor the open structure of cyberspace might have for social struggles within authoritarian states. In the long run, this serves U.S. interests. Finally, most scholars argue that bilateral or regional conventions on the legal boundaries of cyberspace are deemed insufficient, and as such, a global framework within the United Nations is urgently needed (Nagorski 2010; Lewis 2009). The quest for development of such framework, however, is necessarily permeated by different discourses of power. Hence, a Gramscian analysis seems opportune to capture the significance of this structure.

2.2. A Gramscian Ontology of International Relations

When it comes to the question of ontology within the study of International Relations, this study will seek to advance a critical realist approach. Critical realist ontology, according to Andrew Sayer, stems from the fundamental distinction of the dimensions of knowledge between the 'intransitive' and the 'transitive' dimension (2000: 10). The 'intransitive' dimension can be said to be formed by the objects of science, the things 'out there' that we put under scientific scrutiny. The 'transitive' dimension on the other hand is what we as human beings make out of these objects. These are the theories and discourses that structure our understanding of the universe. Since these 'objects' serve as constituents of the social world they can also be objects of study, and within social science, they are exclusively so. Although different theories might hold different 'transitive' objects of science, what they are about to describe (the intransitive dimension) is always the same. For example, when humans discovered that the earth was not flat but round, the earth as such did not change its shape. To draw some wisdom from Ian Hacking; there is a difference between the construction of *a thing*, and the construction of an *idea of a thing* (Hacking 1999).

In other words, what changed in the discovery that the earth was round was actually the social world. As such, the social world (the transitive dimension), unlike the intransitive dimension, can never exist independently of knowledge. But neither is reducible to the other.

Causation in a critical realist view is not simply 'cause' and 'effect' as according to the positivist view (Sayer 2000: 14). Causation is "the 'causal powers' or 'liabilities' of objects or relations more generally their ways-of-acting or '*mechanisms*'." (Original emphasis) (Sayer 2010: 104-105). In Sayers words: "Causal powers and liabilities may thus be attributed to objects independently of any particular pattern of events; that is, not only when 'C' leads to 'E', but also sometimes when 'C' does not lead to 'E'." (ibid.: 105; See Kurki 2007). The reason behind our positivist tendency to view causation in a successionist way is because most experiments are conducted within 'closed systems'. This is where the consistent regularities take place (Sayer 2010: 14-15). A critical realist view of causation recognizes that the world has ontological depth, and is not mere events: "events arise from the workings of mechanisms which derive from the structure of objects, and they take place within geo-historical contexts." (ibid.: 15). The latter is known as conditions, however, these shall not be viewed as inert but rather as other mechanisms which in their turn have liabilities towards other conditions (Sayer 2010: 107). Therefore, it shall be clearly emphasized that the relationship between causal powers and mechanisms is *contingent* (ibid.).

Reality is further divided into three epistemic categories called domains: *the real*, *the actual* and *the empirical*. First of all, *the real* is defined according to two basic constituents. It is whatever social or natural existence regardless of our experience or intelligibility of it (Sayer 2000: 11-12). Secondly, it shall also be emphasized that the domain of the real consists of objects and their structures and powers. A 'power' within critical realism is identified as something close to a 'potentiality' (ibid.). It may exist even if not exercised. Once again, the objects of the domain of the real might be social like 'state' or physical like 'oil', the point is that they have certain capacities of behavior and causal liabilities towards other objects. For an IR-relevant example, 'sovereignty' might be something that 'exists' even though we cannot find any activity to ascribe its cause, it might exist as a 'passive power', unexercised although existent.

Further, the domain of *the actual* refers to what actually happens when the structures and powers of objects are actualized in 'events' (ibid: 12). As in the previous example, sovereignty in the sense of a 'passive power' is equivalent to the domain of *the real*, while its actual enforcement through exercise of sovereign authority or deployment of military troops to enforce borders can only be accounted for in the domain of *the actual*.

Last of all, we have the domain of *the empirical*. This domain equals our experiences of the world, this can refer to the real and the actual alike but is contingent on our knowledge of them. This means that *observability* is not the only criterion for the existence of particular objects. Structures that may be unobservable can still enter the existence of our knowledge through observation of effects which can only be caused by the existence of such objects (ibid.: 12).

The ontology of critical realism is also cumulative. By this I mean that every domain of reality encompass an aspect held by the ulterior level. At the domain of the empirical we find only *experiences*. The actual encompass *experiences* and *events*. And finally, the real covers *experiences*, *events*, and *mechanisms* (Bhaskar 2008: 13).

In terms of international relations theory this enables us to conceptualize phenomena such as 'sovereignty' or 'governance' at different domains of ontological reality. We might just as in the example above differentiate between a sovereignty of the real, actual, and empirical. The relevance of such separation lies in the systematization of the intelligibility of its nature. It enables us to differentiate between the structure of the underlying mechanisms, the case of events actualizing the powers of these mechanisms, and how it finally impacts our world of politics at the level of experience. This in turn may inform or have causal liabilities towards the mechanisms creating it in the first place, and so on. The relationship between the three domains can therefore be said to be *dialectical*.

Further, the existence of such mechanism does not necessarily point towards a trans-historical logic of the social. This thesis seeks to apply a sociological perspective which is sensitive to historical circumstances that might determine outcome of dialectics rather differently in different contexts (Barkin 2010).

Hegemony, as defined by Antonio Gramsci has such a feature (Cox 2002; McNally & Schwarzmantel 2009). Central to Gramsci, was that material conditions (the real) must always be taken into account when analyzing the social and the process of formation (the actual) within *historical blocs* (ibid.: 168). However, since the importance of dialectics should be stressed, *the actual* also have the power to refigure *the real* in various ways. The notion of 'hegemony', in Gramsci's terms, should be understood as a general consent between the dominant social force and subaltern social forces which results in a conformity of behavior in line with the interests of the dominant social force (ibid.: 164ff), in contradistinction to dominance based on coercion (Moolakkattu 2009: 441).

A meaningful definition of the state therefore has to include not only the state apparatus, but also its underpinnings in civil society, such as "the church, the educational system, the press" and other institutions facilitating the hegemonic social order (ibid.). Hegemonic orders change through the revolutions of social forces, and usually move across nation-state boundaries to transform the relations of social forces in respective contexts through what is known as *passive revolution* (ibid.). This means that the predicament for change is not anchored in the social forces of these respective contexts but rather imposed from above by *trasformismo*. *Trasformismo* is a strategy of "domesticating" ideas shaped by social revolutions of another order, and potentially make them 'less dangerous' to the particular order (ibid.).

A hegemonic world order in these terms is therefore to be understood as phase in history when the economic, social, and cultural institutions, as well as the technology of a hegemonic order become models for emulation globally (ibid.: 171). This process takes place within peripheral regions of the world, as a *passive revolution* (ibid.). This thesis will use these concepts to determine the contemporary and possible future structure of such a hegemonic world order within the contours of cyberspace, as it might emulate from the U.S. model (McEvoy Manjikian: 386). The next section will introduce my formula of securitization.

2.3. Securitization Theory – A 'Hermeneutics of Security'

Securitization theory (henceforth ST) within IR comes in many different guises. This study will utilize a composition of sociological and hermeneutical approaches' towards the process of securitization. The sociological perspective is developed by Thierry Balzacq (2010). According to Balzacq, the most basic assumption within ST is "the insight that no issue is essentially a menace." (ibid.: 1). Balzacq´s sociological perspective differs from a philosophical use of this theory – as within the Copenhagen School – which emphasizes 'performativity' of language. He argues that it is a rather philosophical approach that does not pay sufficient attention to historical/regional/sectorial contexts' and relations of power (ibid.: 1-3). The sociological version of ST on the other hand put emphasis on the power of the agents involved in the process (ibid.). Another remark against the Copenhagen School is the rather contradictory definition of security as both a 'speech act' (i.e. performative construction) *and* 'survival in the face of existential threats' (i.e. fixed meaning), as is fastidiously noticed by Felix Ciută (2009). This study will abstain from this second meaning and seek a 'hermeneutics of security' concerned with the meaning of 'security' ascribed by the object of study (ibid.). Another relevant critique of securitization is its claim of describing 'new' dynamics in the field of security. In the case of the U.S., some argue that economy and security for example has always been indissociable concepts (Phillips 2007).

A 'hermeneutics of security', in terms of analytical focus, is concerned with five mutually reinforcing dimensions of securitization: the construction of *threats*, the construction of *referents*, the construction of *securitizing actors*, the construction of *security measures*, and the construction of the *meaning of security* (ibid.: 317). This repertoire of hermeneutical tools fit well within Balzacq's model apart from one – should be for constructivists – important feature; the contextual *meaning of security*. Nonetheless, apart from that, Balzacq's theory is of central relevance to this thesis. It first of all emphasizes that securitization is not to be understood as a "self-referential practice" but rather an "*intersubjective* process" (ibid.: 3). The primary constituents in the process of securitization are *agents*, *acts*, and *context* (ibid.: 35-36).

As for *agents*, *referent objects* are those things that are "seen to be existentially threatened and that have a legitimate claim to survival." (ibid.: 35). *Securitizing actors*, in turn, are those actors that initiate the securitizing act by uttering the word 'security' and allocates it to a referent object (ibid.: 35). Intermediate within this process are the *functional actors*, those that "affect the dynamics of sector." (ibid.: 35).

Secondly, when it comes to *acts*, both discursive and non-discursive practices need to be analyzed. These practices also have four facets: *action-types*, *heuristic artifacts*, *dispositif*, and *policy* (ibid.). Plainly speaking, what Ciută by contrast, rather comprehensibly refers to as "security measures" (2009: 317). *Action-type* refers to the appropriate language used to perform a given act, its syntactical and grammatical rules. *Heuristic artifacts* refer to strategic resonance used by the securitizing actor for creating the circumstances for mobilization of the audience (ibid.). *Dispositif* refers to the "constellation of practices and tools" utilized for securitization (ibid.: 36). The so called "tools" are generally of two kinds: *regulatory instruments* and *capacity tools* (ibid.: 17). *Regulatory instruments*, which is an impingement of 'governmentality', aims to "normalize" the behavior of subjects - such as a policy (Balzacq 2011: 17). *Capacity tools* on the other hand are objects operating within the framework of policy, different types of modalities such as forces and resources to attain the purpose of policy (ibid.). The fourth and last facet of this level of study is *policies* generated by securitization (ibid.: 37). This thesis argues that this facet is unattainable at the particular moment. Since the object of study is the *Cyberspace Policy Review*, it is far from certain if the proposals of this policy review will be reflected in the actual policies. Therefore, the hermeneutic ambition of this study can at best locate a predicament for the potential policies of securitization rather than capturing the process in all its features.

Last of all, the level of analysis concerned with *context* takes departure from the assumption that "discourse does not occur nor operate in a vacuum; instead, it is contextually enabled and constrained." (ibid.: 36). Context includes modes of production, class structure, and political formation. This can be analyzed in two aspects owing to a distinction between *distal* and *proximate* contexts. The *proximate context* is similar to what Erving Goffman refers to as a 'setting' (Goffman 2009: 25ff), the genre of interaction that determines the rule of a specific occasion, such as a meeting, summit, and in this particular case: a policy review assessment. The *distal context* by contrast is composed by the sociocultural embeddedness of the text, the identity of the actors, and the institution where discourse occurs. Balzacq stresses the recursive effects of these factors (Balzacq 2011: 37).

In this particular case, this focus will concern the governmental role of participants in the assessment of the policy review. Returning to Ciută, this dimension of analysis must also encompass a normative evaluation of practices and concepts constructed within the policy of security (2009: 324).

3. Methodology

3.1. Choice of Method

This thesis has chosen to analyze the empirical material through a method known as *critical discourse analysis* (henceforth CDA). This choice stems from the material available for analysis. Most data on the *actual* cases of cyber warfare or other types of events when the concept of sovereignty, violence, and governance might come into question is classified information (Heickerö 2011: 9), therefore disqualifying many facets of useful quantitative methods on the basis of inaccessibility of required data. This choice also draws from the advised methods of analyzing securitization as mentioned by Balzacq. He prefers the analysis to be conducted by discourse analysis, ethnographic research, process-tracing, or content analysis (2011: 39-53).

Discourse analysis proved most utilizable in this case since the meaning of 'security' is successfully captured by this approach (ibid.: 39). Ethnographic research would be boundless as a matter of scope in this analysis since I study the process at a macro level (ibid.: 44), and as such don't pay much attention to the 'popular audience'. Process-tracing on the other hand would capture this macro-level chain of events rather firmly (ibid.: 46). However, this would make the thesis diachronic rather than synchronic (See 1.5.). Last of all, content analysis under-emphasize the social aspects of text and therefore disembark from the sociological approach used in this thesis (ibid.: 50).

Another argument for pursuing a qualitative approach is that the so called 'events' in need of investigation are often 'unobservable'. But through a qualitative CDA I am able to analyze the governmental imperatives that regulate or *structure* the activities of states in the domain of cyberspace. The most fundamental flaw in this qualitative approach with the criteria of empirical material chosen for analysis is that it will not investigate *de facto* cyber governance, but rather cyber governance *de jure*. The analysis is directed on the policy itself rather than its actual application. I am well aware that an all-encompassing analysis would in fact require a triangulation of both quantitative and qualitative methods (See Esaiasson et al 2007; Sprague 2005). This includes some data on actual cases of state warfare within cyberspace, the identity of actors, and so on. The reason for exclusively analyzing the *Cyberspace Policy Review* and no other document is that it is a general policy assessment which collects all of the major policy areas concerned with cybersecurity. A specific policy document would limit the analysis and would not suffice to capture the process in all its features.

3.2. Qualitative Method & Critical Realism

The strength of quantitative methods is their degree of standardization of procedures (Sprague 2005: 81). Qualitative methods on the other hand are valued for their capability of acquiring scientific depth through the use of interpretation (ibid.: 119). CDA is such a method. It differs in crucial ways to other kinds of discourse analysis, as in the discourse analysis of Laclau & Mouffe (2001) for example. The main difference stems from their differing approach towards the question of ontology. Norman Fairclough, which is the originator of this method, holds a critical realist (CR) perspective on ontology (Fairclough 2003: 14).

Ontology from the perspective of CR might be described as realism drawing upon the influence from the *linguistic turn* in social science (López & Potter 2005: 6-8). As was assessed in section [2.2.], CR acknowledges that there is a world outside of our discourse of construction, but that our knowledge and access to this 'outside reality' is limited. However, we still need to always acknowledge the *possibility* of its existence (Bhaskar 2008: 21-30). For this reason, we must always strive to improve our ways of accessing reality by seeking 'inquisitive' methods of social science.

I argue that this epistemological process is best accomplished by use of *retroduction*. This is the procedure of reasoning as has been spelled out by Andrew Sayer (See section 2.2.). *Events* are explained by the assumption of the existence of *mechanisms* which have the power of producing them (Sayer 2010: 107). The mechanism might be known beforehand, or else it might be hypothesized (ibid.). A mechanism can exist even if its powers are not deployed at the precise moment.

3.3. Critical Discourse Analysis

Norman Fairclough applies this theoretical framework of critical realist ontology onto his textual analysis (2003: 14). The three domains of knowledge - the real, the actual, and the empirical - (Bhaskar 2008: 13) are subsequently translated into *social structures* (the real: mechanisms, events, and experience), *social practices* (the actual: events and experience), and *social events* (the empirical: experience) (ibid.: 23-25, 36-38). Social structure in this case is *languages*. Social practices are what Fairclough refer to as *orders of discourse*. And social events are *texts* (ibid.: 24). Their relationship to each other is *dialectical*, in which the 'orders of discourse' function as *intermediate* (ibid.: 25-27). Each and one of them are also further differentiated. A discourse within social practice figures in three ways. As: *ways of acting* (genres), *ways of representing* (discourses), and *ways of being* (styles) (ibid.: 26). Text is also categorized according to function or *meaning* in correspondence to the former typology: *action*, *representation*, and *identification* (ibid.: 27). Last of all, we also need to pay attention to semantics, grammar and vocabulary, and phonology/graphology as having separate 'internal' functions within texts (ibid.: 36-37). Phonology and graphology however, is not put under attention in this thesis.

If we acknowledge these theoretical assumptions we may also adopt a perspective were we identify causal powers embedded in texts that might cause events taking place 'outside' of the text (Fairclough 2003: 8).

The main criticism against CDA is its tendency to blur the distinctions used and that it does not actually analyze how a text can be read in various ways (Blommaert & Bulcaen 2000: 455ff). It confuses signification and significance as well as pragmatics and semantics. As such, critics hold it to be deterministic. It projects the political biases of the analyst onto the data (ibid.).

3.4. Operationalization & Analysis of Data

As is emphasized by Balzacq, the main attention in a discourse analysis of securitization should be directed towards representation, heuristic artifacts, and the kind of interactions generated by the process. Therefore, the concepts of importance in terms of operationalization are *actors* and their representation, the *act* in terms of heuristic artifacts and dispositifs, and the *context*.

Actors are identified in the empirical analysis as every use of pronouns such as 'our', 'we', 'their' and so on, but also by direct reference to specific units such as 'the Nation', 'the American people', 'the White House' and so on. All of these are dedicated different functions within securitization according to the differentiation between referent objects, securitizing actors, and functional actors. These are subsequently identified within chains of potential causalities within the text, and how they are modalized. Such as, X 'should' do Z to Y. High modality is identified when the text express total certainty, indicated by explicit use of archetypal markers such as 'it is' or 'are' (Fairclough 2003: 68). This is put in contradistinction to 'low' modalities such as 'it may' or 'can'. The function of explicit modalities in this case is outlining commitments to truth (epistemic) or obligation (deontic), what the authors commit themselves too (ibid.) (See Annex 6). In order for the analysis of my data to become successful I had to break down my inquiry into operationalized questions that would enable a conceptualization of the analyzed phenomenons. The questions entailed:

What is the contextual meaning of 'cybersecurity'?

What is the action-type of the text?

What is the distal context of U.S. cyberspace governance?

How is 'governance' represented in the CPR in respect to 'state', 'market', 'civil society', and 'international community'?

How are referent objects, securitizing actors, and functional actors expressed in terms of identification and representation in the CPR?

What degree of modality is used? (Regarding all levels of analysis)

Which are the actors contributing to the assessment of the CPR? (Enclosed in Annex 1)

How is the interest of respective actors represented in the CPR?

What heuristic artifacts and dispositifs are represented in the securitizing acts of the CPR?

How are procedures legitimated?

During the analysis of the text, I used a procedure of coding of my own invention. I started by marking all modalities with a certain color throughout the document. The modalities was then allocated the status of being either epistemic or deontic, and sorted by level of degree. I proceeded by marking all of the actors in another color, followed by an analysis of evident assumptions (See Annex 4).

To make the identification of dispositifs compatible with Gramscian notions I also allocated the 'sphere of interaction' and 'legitimation' (authorization, rationalization, moral evaluation, or mythopoesis) (See Annex 6) of these measures, that is to say, by whom towards whom they are deployed, and how, which is central to understanding the triad struggle of society as a *war of positions* (2010: 238-239).

I then went on to mark narratives of threat, intertextualities, and grammatical relations of sentences which ascribe to certain rules of language. Such as semantic relations concerning whether claims was causal, conditional, temporal, additive, elaborative, or contrastive (Fairclough 2003: 89ff) (See Annex 3). As time lagged, I eventually ended up conducting this procedure exclusively on the passages that was relevant for the other facets of the analysis (See Annex for analytical and coding schemes).

3.5. Methodological Problems

When conducting social science it is always important to keep in mind the *validity* and *reliability* of the study in question. In terms of the CDA utilized in this study it means, in first instance, that all of the assumptions underlying the method should be as *intersubjective* as possible (See Gilje & Grimen 2007: 23). If it can arguably be proven that there exists a causal relationship between the analyzed text to the events taking place at the macro-social level (what is assessed from previous research); then it can be concluded that this study hold some validity. One criterion with which to establish some validity is to follow the method as described by Fairclough as strictly as possible. In that case the thesis can lean against the inter-scientific credibility of the paradigm itself. But in the end, the epistemological and ontological assumptions that underlie the theory of Fairclough's model (See 2003: 3ff) have to at least be entrusted in order for the study to be of valid relevance.

In the second instance we encounter the problem of *interpretation* (ibid.: 190ff). It is unclear whether my interpretation of a specific thing will correspond to the interpretation of others. Hence, the study may encounter problems of *reliability*. Some support in this regard is derived from the linguistically systematic character of critical discourse analysis itself. This enables the method to exhaust the texts rather successfully without the use of too much subjectivity.

As is emphasized by Gilje & Grimen there is after all no correct interpretation of a text. A text is always more or less credible (ibid.: 198ff). Returning to the initial two inquires of this paper: how governance is represented in U.S. cyberspace policy and if it is possible to identify a process of securitization within U.S. cyberspace policy? The main problem here is that of theoretical confusion regarding how the concepts are understood from within a different context. In this case, I think social science must content with Nietzsche's known fact: "only that which has no history can be defined" (Bartelson 1995: 13).

To hold some humility towards the text, and how the identity of its authors, might affect the formulation of the text; I always kept a Derridean mantra close at hand (Derrida 1979). That means, every time I stumbled over sentences such as 'I have forgotten my umbrella'; I kept in mind that sometimes people spell wrongly, sometimes they have a bad (or good) day, and some peculiar formulation at some limited section should therefore not be 'ravaged over'. The CPR even had some grammatical errors, and its style shifted between chapters, I opted to remain humble towards these factors, and not let it carry me away on farfetched speculations.

4. Analysis & Results

4.1. Context - The Cyberspace Policy Review

The document issued under the contemporary administration of the U.S. entitled *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* (henceforth referred to as the CPR) was created as a means to assess policies and structures for U.S. cybersecurity. The executive summary of the CPR states that cybersecurity policy encompasses "strategy, policy, and standards regarding the security of and [sic.] operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions." (Cyberspace Policy Review 2009: i). The CPR is also explicitly focused upon questions of security and is not concerned over other policies on information and communication.

The concept of "cyberspace" in the CPR is derived from the definition as defined by the National Security 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). Cyberspace is "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, and embedded processors and controllers in critical industries." A common usage referred to is also cyberspace as "the virtual environment of information and interactions between people." (ibid.: 1). Therefore, the concept of cyberspace (in the CPR) encompass of not only what we know as the Internet, but a broader category of communication-systems. The importance of cyberspace is highlighted by its relation to utility; as a structure underpinning "every facet of modern society" and especially "the U.S. economy, civil infrastructure, public safety, and national security." (ibid.: iii). This is where the questions of governance enter the picture. The architecture of cyberspace was developed by contemplation over its utility rather than of its security. As the CPR states, the U.S. therefore encounter the "dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights." (ibid.). As will be accounted for in the following chapters, the legitimation of procedures is by large derived from what Fairclough call *rationalization* (reference to utility), and to some extent *authorization* (reference to traditions of authority) (2003: 98). *Moral evaluation* (reference to values) and *mythopoesis* as legitimation through narrative is rather absent apart from some instances (See 4.4.2.) (See Annex 6).

4.1.2. The Contextual Meaning of 'Cybersecurity'

Concomitant from the bold ambition of this thesis to take the study of securitization, in virtue of given contradictions of its contents (See Ciută 2009; Guzzini 2011), back to a hermeneutic understanding of the notion of 'security'; a contextual interpretation is needed (Ciută 2009). Since understanding 'security' is also pivotal to the analysis of governance (See section 4.2.); this interpretation had to be conducted before the different levels of analysis of securitization could be performed (See section 4.3. & 4.4.).

Previous research on the subject has been clear to distinguish between two dimensions, risk *to* cyberspace and risk *through* cyberspace (Deibert & Rohozinsky 2010).

Therefore, 'cybersecurity', in the context of the CPR, is to be understood as a sphere of security encompassing the security dimensions of military, economic, political, societal, technological, and ecological security. The introduction to the CPR highlights "economic and national security interests" (Cyberspace Policy Review 2009: i). There is no mention of 'existential threat', but the two terms highlight the prevalence of the economic-security nexus.

The security strategy and policies regarding cyberspace includes 'threat reduction', 'vulnerability reduction', 'deterrence', 'international engagement', 'incident response', 'resiliency', 'recovery policies and activities', 'computer network operations', 'information assurance', 'law enforcement', 'diplomacy', and 'military and intelligence missions'. All of these words are used rather perfunctory and are, regrettably enough, not satisfactorily defined. Unsurprisingly, this may be due to the genre (Fairclough 2003: 63ff) of the CPR and the potential readers it might attract, such as policy-makers, cyber industry advocates, politicians, and epistemic communities. The meaning of these terms is most likely self-evident to most of these actors. 'Threat reduction' and 'vulnerability reduction' seems to be offensive and defensive proactive strategies of military significance. 'Deterrence' is as every scholar of International Relations knows, an offensive military strategy aiming at deterring adversaries from offensive action. 'International engagement' on the other hand is an evasive term. Since it is distinguished from 'diplomacy', as the standard bilateral mode of political interaction between states; it might just refer to political interaction with international institutions. 'Incident response' in its turn, is widely used throughout the CPR. In most instances, it is referred to as a reactive military and political practice to safeguard societal security. It is for example used in analogy with "natural disasters" and "terrorist attacks".

‘Resiliency’ is devoted equal diligence, but on the other hand, it cannot decisively be located as a strategy or policy of security but rather as an ontological structure of cyberspace (ibid.: 29). Further, the term ‘recovery policies and activities’ is represented as a ulterior category to ‘computer network assurance’, ‘law enforcement’, ‘diplomacy’, and ‘military and intelligence missions’. This seems to concern the integrity of the operation of these activities and can therefore be reckoned to cover economic, military, political, societal, and technological security. Unsurprisingly enough, cybersecurity seem to cover the whole array of other security dimensions by virtue of its causal liabilities among objects at a global reach (ibid.: iii).

Subsequently, *cybersecurity* – in the discursive construction crafted within the CPR – can conclusively be interpreted as according to the prefatory formula in this chapter; as a *domain* of security encompassing all of the *dimensions* of military, economic, political, societal, technological, and maybe even ecological security. This might seem far-fetched, but the CPR itself invites for such interpretation in one single instance where cyberspace is called a ‘global trusted eco-system’ (ibid.: 34). This is not totally intelligible if – and only if – the discourse of cyberspace as a ‘global common’ is invoked. Then one could think of it as having a similar function as the high seas, difficult to enforce with boundaries and necessarily interconnected. Not to mention the causal liabilities of energy grids and cyberspace, and the effect a nuclear disaster have for the environment. If cyberspace is to be viewed as a global common is also left undecided by the CPR, but it do raise the question (ibid.: B-4), and as such, it has entered the contours of cyberspace discourse The next section will outline the significance in terms of action-type of the CPR.

4.1.3. The Action-type of the Cyperspace Policy Review

The most common prevalence of imperatives in the CPR is ‘should(s)’, they amount to 127. These are followed by the 62 ‘can(s)’, 50 ‘will(s)’, 34 ‘would(s)’, 33 ‘may(s)’, and 27 ‘must(s)’. These are all ‘deontic’ modalities of commitments to obligations from the part of the CPR (Fairclough 2003: 168). The overall level of degree to the deontic modalities is median leaning towards high (ibid.: 170). As for the ‘epistemic’ modalities, it is significant that the ‘will require(s)’ outnumber the ‘may require(s)’ (See Annex 2). Likewise, the aggregate epistemic modalities are expressed as high. In conclusion, the CPR is highly declarative and imperative. The significance of this might be that the CPR has the function of being ‘orders’ or political suggestions. And these have highest priority in terms of its role in ‘causing’ securitization.

4.2. Governance & Relations of Power

As is central to a Gramscian analysis of International Relations, the social forces and modes of production are key to the intelligibility of the hegemonic discourse and the structure of the state (Cox 1983). This section aims to, in broad strokes; outline these features as they are understood from the formulations within the CPR.

4.2.1. Contextualizing U.S. Cyberspace Hegemony

Following the theoretical presumptions of this thesis, social forces and the mode of governance deployed are necessary factors for the intelligibility of any rationale for securitization. Frugally stated, securitization cannot be a goal in itself, but rather a means to an end. Social forces, and their production of discourse as dialectically influenced by material conditions, necessarily underlie such means. Thus, a contextual approach informed by theoretical guidance that clarifies (or simplifies) social relations, material conditions, and their synchronic constellation is humbly motivated. This does not mean that they are captured as '*ding an sich*' in analysis of a policy review, but it do capture the discourse of hegemony, in which they are constructed as the thought-of-as (prospective) subjects of governance.

The *distal context* in which the process of U.S. hegemony in cyberspace is written, takes place within a liberal-capitalist global order currently undergoing far-reaching changes (Bromley 2003: 67). These changes are characterized by an increasingly interdependent dynamic between territorial centers of political power, especially the United States, China, and the Russian Federation (ibid.). The Internet, as having its place of birth within the United States might be regarded as one of the pillars underpinning the hegemony of the United States and a transnational capitalist class intrinsic to its economy (McEvoy Manjikian 2010: 384). As for the mode of production, the Internet as we know it is a crucial factor underlying the JIT-systems within post-Fordist production (Castells 2001: 77ff). In Gramscian terms, it has allowed the United States to impose a *passive revolution* worldwide (as far as the technological capacity for connectivity is concerned) for the adoption of economic, cultural, and political values, and technological means to promote its hegemonic mode of production.

Such an interpretation finds some support in the CPR, but not too decisively. The CPR is even concerned over the contemporary structure of cyberspace. The information and communications sector is increasingly merging into a common infrastructure. This means that formerly 'closed' systems such as tele-communications are now connected to the wider Internet. This dawning cyberspace is of a decentralized nature which "allows individuals and entrepreneurs to develop and deploy innovative applications at the edges of the network without obtaining permission." (Cyberspace Policy Review 2009: 31).

This may, notwithstanding its substantial hegemonic function, indicate concern over cyberspace as being 'ungoverned', as is usually the representation of cyberspace by realist schools of thought. Consequently, in such a horizontal environment, no actor are "' [...] prepared to take responsibility for end-to-end systems design.'" (ibid.: 32).

Further, another trend is the "movement of data and services to third-party network-based servers" (ibid.), or what is usually referred to as 'cloud computing'. This means that data is increasingly stored on connected cross-boundary spaces instead of inside single hard drives. The challenge deriving from this development, in the view of the CPR, is its spread "across jurisdictional boundaries" with consequences for law enforcement and privacy and liberties protections, as they are defined differently across countries (ibid.).

But nonetheless, in terms of McEvoy Manjikian's typography of views (2010: 387**)**, the CPR leans further to a liberal than a realist view. The *structure* at this particular moment is perceived as decentralized and market-determined, in line with a liberal view (Cyberspace Policy Review 2009). The actuality of cyberspace based upon this structure is subsequently characterized by a constant tension of contradictory dynamics, where some actors seek to limit the impact of data movement while others (with multinational operations) seek to take advantage of geographic and time-zone diversity (ibid.: 32).

The current strategy of the U.S. as elaborated in most sections of the CPR is concerned with daily practices of the *cyberspace actual*. In one section however, a proposed "focus on game-changing technologies" (ibid.: 32) will seek to restructure the *cyberspace real*. This includes a moving away from Internet Protocol-based networks for critical infrastructures such as the U.S. power grid (ibid.). Such a restructuring would be significant because it would change the very operability of the system. It would be a non-discursive solution, in contrast to most of the discursive realignments proposed in the CPR.

In conclusion, the contemporary *distal context* of cyberspace does in fact not adequately convey U.S. hegemony, the benefits of an "environment that promotes efficiency, innovation, economic prosperity, and free trade" do not seem to outweigh the perceived need to enhance 'security' and 'resiliency'. And that is obviously enough the underlying predicament for the rationale of initiating a structural change. But the solution is not a realist one, it is liberal.

4.2.2. The Subjects of Cyber Governance

In this section, the subjects of governance as outlined in the CPR (Cyberspace Policy Review 2009) will be examined. First of all, when it comes to the vocabulary used to represent the state, some of the following was used: ‘the government’, ‘the Federal Government’, ‘federal departments and agencies’, ‘The President’, ‘the White House’, ‘the Constitution’, ‘the United States’, and specified units such as NSC, NEC, EOP, CIA, DNI, NSB, NIST, ICI-ICP, HSC, OMB, CNCI, OSTP, NSTAC, NIAC, CIPAC, ISPAB, PCLOB, JIACTF, CIOs, CISO, NSF, FAA, DARPA, and NSTC (see list of abbreviations).

According to the CPR, more than 20 federal departments and agencies are at the moment vested with overlapping responsibilities for cybersecurity operations. The overall critical infrastructure protection defensive strategy efforts is under *The National Strategy to Secure Cyberspace of 2003* and *HPSD-7*, assigned to the Secretary of Homeland Security as a coordinator (ibid.: 4). An evident conclusion derived from the discursive analysis of this section is that a central coordination is lacking in the contemporary efforts. This is indicated by reference to a strategy from 2007 by the *Comprehensive National Cybersecurity Initiative* (CNCI), which proposed a “bridging” of formerly decentralized missions within the Federal government into a centralized chain of responsibility. The “bridging” covers an interlocking of law enforcement, intelligence, counterintelligence, and military capabilities within Executive Branch networks. Consequently, these capabilities are still only used to protect ‘governmental’ communication infrastructure. And is therefore limited in the ambition of securing ‘U.S. cyberspace’ (including non-governmental critical functions), which seems to require a global endeavor. Consequently, sovereign responsibilities are limited almost exclusively to state digital infrastructure, and does not encompass ‘industry’ and ‘civil society’. The interconnectivity of cyberspace highlights a focus on *dependency* (ibid.: 5). ‘National security’ in this case cannot be viewed as concerned solely over objects of U.S. property or possession. It is more like with the case of rivers, what happens upstream is as important as what happens within the boundary of possession.

In conclusion, overall governance over cyberspace, as interpreted from the analysis of the CPR, is therefore not strictly concerned with boundaries. It subscribes to post-Westphalian logics, similar to the concept of ‘Empire’ as a form of governance (See Bromley 2011). This highlights a concern from the U.S. administration that if governed too tightly, it will neither work nor gain any legitimacy; in line with the liberal view. It is a mode of ‘governing without smothering’.

4.2.3. Governing the State

The first proposal by the CPR for sorting out the question of governance is the creation of a *central coordination mechanism* within the "White House" (Cyberspace Policy Review 2009: 7). The function of this mechanism, which is an individual cybersecurity policy official (henceforth the CPO), will be to *harmonize* competing policies into a 'national policy' of cybersecurity (ibid.). In other words, it seeks to create an officer of discourse.

Performance of *operational roles* is proposed to remain in the departments and agencies currently vested with these powers (ibid.: 8). The accountability of departments and agencies to perform these operational roles is although put under question. This is indicated by the proposed need for strengthened legislation to hold leaders of departments and agencies accountable to these responsibilities (ibid.: 11). In case of an actual significant cyber incident, it is also the case that the authority of coordination rests within the White House. In this instance, the CPO functions as "the White House action officer for cyber incident response" (ibid.: 23). This means that the *strategic* authority for cyber governance is vested within the White House.

This imperative illuminates the relation between *law* and *policy* within U.S. governance. Although the activity of departments and agencies is enshrined in clearly defined laws, the intervention of policy might function as an instrument of power to make them further subjected to the White House in a more subtle manner. The issue is concerned with compliance with the cybersecurity policies. This analysis subsequently holds it as a possibility that the purpose of 'policy-compliance', as opposed to changes in law, is a shortcut around legislative efforts which is mainly absent as a matter of solution to the current issue. Legislative efforts are Constitutional matters, while policy, know no judge but the potential CPO. However, as is stated with a low degree of modality, any consolidation into a unified structure of cyber response "may require" legislative means (ibid.: 23). At the moment, it seems to be at least three separate structures to govern, each with responsibilities for their own networks. The Defense Department, the Intelligence Community, and the United States Computer Emergency Readiness Team (US-CERT) with responsibility over civilian federal agencies and some private sector partners (ibid.: 24).

In conclusion, the policies concerning governing cyberspace operations within the state apparatus is more focused on creating and enforcing upon agencies a hierarchy of policy centered within the White House, and does not encompass any particular changes in law (at least not in the CPR, although it clearly highlights the possibility of such necessity). Regarding the consequences of this model, it might be presumed that it can lead to a very 'flexible' structure. One advantage for the contemporary administration could be to facilitate changes in policy. On the other hand, when the administration is replaced through elections, it would necessarily be equally easy to reformulate the policy at hand. It would practically amount to replacing the CPO. And as such, it could, in terms of politics, prove to be quite maneuverable a system.

4.2.4. Governing the Market

The state-market relation in the focus, from the part of the CPR, is aimed at a corporativist form of governance, persistent by the far-reaching entanglement between society's critical functions and the corporate ownership of 'industry'. Telecommunications, electric power, energy pipelines, refineries, financial networks, and other critical infrastructures are considered vulnerable from attacks from other nations without the use of kinetic force. Criminal activity is also assessed as having caused a loss of intellectual property worth of one trillion dollar during the year of 2008 (Cyberspace Policy Review 2009: 2).

The first facet of the public-private partnership is captured within the term of "enterprise leadership responsibility" (ibid.: 28). This include information sharing on "threats, vulnerabilities, and effective practices" between government and industry. In terms of a synergy of interests, this is referred to as a "shared responsibility" between the public and the private sector. "Business" and "government" is represented as spheres of equal nature, dependent upon each other. And no monopoly of violence within the contours of U.S. cyberspace is ever proposed. Crux of the matter concerns the question of sovereignty:

> The common defense of privately-owned critical infrastructure from armed attack or from physical intrusion or sabotage by foreign military forces or international terrorists is a core responsibility of the Federal government. Similarly, government plays an important role in protecting these infrastructures from criminals or domestic terrorists. The question remains unresolved as to what extent protection of these same infrastructures from the same harms by the same actors should be a government responsibility if the attacks were carried out remotely via computer networks rather than by direct physical action (ibid.: 28).

An explication of the proposed structure of cyber sovereignty is given in which the use of "the country" is used to represent 'territorial' sovereign responsibility of the federal government. It is also concerned with state or regime security by reference to the defending of "all levels of government" and ensuring citizen safety and well-being. Nonetheless, since the 'territory' at question, namely the digital infrastructure, is "designed, built, and operated by the private sector", the CPR is clearly revulsive towards making the same claims towards private networks (Cyberspace Policy Review 2009: 17). It is therefore a 'sovereignty of interdependencies' with shared governmental-corporate responsibilities, or maybe not sovereignty at all. The model includes some changes in law, but especially within policy (soft law).

One such measure is the development of "threat scenarios and metrics" that can be used for risk management, recovery planning, and prioritization of R&D. This measure requires the private network operators to inform government about sophisticated intrusions (ibid.: 24).

The question at issue is referred to as "limitations of law enforcement and national security" (ibid.: 17). A strategy to create incentives for these commitments is to assign the consequences a monetary value for business to take into considerations in their corporate risk management. They are encouraged to take upon "collective risk". Such public-private partnerships already exist, but suffer from "unclear delineation of roles and responsibilities" according to the CPR (ibid.: 18).

Barriers to such measures is expressed by the private sector as "'collusive' or contrary to laws forbidding restraints on trade." (ibid.: 19), as well as concern to share sensitive business information with government in fear of "reputational harm, liability, or regulatory consequences" (ibid.). In other words, the mere existence of 'information sharing regimes' (ISRs) might give governments insights about areas in need for further regulation, which is a fundamental concern for the 'private sector'. Another concern for the private sector is that incident reporting may also risk market reactions with negative causal impacts from the actions of shareholders (ibid.).

But the issue also runs in the opposite direction, namely as a governmental concern in sharing sensitive intelligence information with the private sector, which might endanger "the privacy rights of individuals." (ibid.: 19). This concern is expressed by the "civil liberties and privacy community" (ibid.). The CPR echoes of this concern in the strongest possible modality. For example, "the government must protect privacy rights," unlike most other references to commitments which is modalized by the use of "should" (ibid.: 26).

The proposed solution by the CPR seems to be something of a trade-off were issues that might threaten governmental public legitimacy or national interest is vested within the state while all other activities remain under the authority of the private sector. For example, institutions central to U.S. hegemony, such as The World Bank and the International Monetary Fund; ‘should’ be assisted with information, and encouragement of “best practices”. ‘Public legitimacy’ is incident to securing health, energy, and transportation, as they are fundamental to matters of protecting patient information, penetration or large-scale attacks on energy-related industrial control systems, and air trafficking control systems (ibid.: 28). Protection of networks on the other hand is proposed to remain, by their own will, in the hands of private network operators. The model for cyber governance, just as in its current form, therefore takes upon a rather corporativist structure that overrides strictly economic concerns, corporations enjoy a certain amount of autonomy on the use of cyber violence. It is a ‘free market of violence’ rather than a monopoly of violence.

In sum, this model of governance seems to highlight the complex relation between government and corporations within areas of security in a globalized world. For example, since many global corporations operating within the U.S. is foreign owned, it might be problematic to include them into a sphere of sovereign protections and ISRs. Current antitrust laws, as stated by the CPR, prevent such measures since it would create unfair competition in regard to solely national corporations.

One proposed solution is therefore the establishment of a non-profit non-governmental organization as a “third-party host” for ISRs (ibid.: 26). Another proposition is regional or local partnerships between state, local and tribal governments and individual or groups of firms for limited but voluntary ISRs (ibid.). In order to create legitimacy for such measures, the CPR elaborates on a market-based incentive mechanism. Corporations can be provided governmental protection in exchange for reduced liability or entrust themselves with protection in exchange for increased liability (ibid.: 28).

In conclusion, the governance of private cyberspace remains voluntarily in their own hands. It includes strengthening of a state-market nexus by encouragement of cooperation, not by sovereign subordination of the latter under the forces of the former. The fundamental issue of ‘sovereignty’ and ‘monopoly of violence’ as has drawn much attention from academia and policy-makers is, with the structure of cyberspace as accounted for in chapter [4.2.1] borne in mind, perhaps not as insoluble an issue as has been presumed.

4.2.5. Governing the Civil Society

As for the commitments of the "general public" (civil society) the CPR outlines a discursive strategy of *raising awareness* (Cyberspace Policy Review 2009: 13). The strategy is twofold. First of all, it aims on expanding university curricula and prioritize math and science within public education. The explicit purpose of this is to create a workforce which can support future development of the information and communications industries.

Secondly, the CPR proposes nation-wide awareness campaigns to create 'appropriate ethics' in cyberspace. An interesting feature is that the agent behind this program is not referred to as the "White House" or "government" as was the case of the previous spheres of governance (state and industry). Rather, the use of "the Nation" is deployed in vocabulary, indicating a different approach.

The term *hegemony* is suitable in this instance since the state (the state-market nexus as was outlined in the previous subsection) aims to control the general public by mobilization of appropriate ethics for risk management, which is probably in line with the hegemonic interest of 'governing without smothering'. Presumably, this strategy is vital as a matter of governance since any extended governmental authority over civil society would stand in conflict with the interests of maintaining "innovation, open interconnectivity, economic prosperity, free trade, and freedom while also ensuring public safety, security, civil liberties, and privacy." (ibid.: 13).

The agent supposed to initiate this awareness program, previously referred to as "the Nation", is the "Federal government in partnerships with educators and industry" (ibid.). Consequently, the concept of 'Nation' can be presumed not to include civil society in this case, since civil society is the object of, rather than subject behind this program. The program is proposed to be headed by the CPO with the endorsement of Congress, State, local and tribal governments, the private sector and the civil liberties and privacy communities. Such a list of endorsements indicates the apparent need for legitimacy for such measures.

The transitive objects or elements under question are "digital safety, ethics, and security." (ibid.: 14). As such, the CPR makes a different distinction as regards the elements of policy exclusively for civil society, compared to other spheres of society. The market for example does not seem to be in need for further ethics. Nonetheless, digital safety seem to include "responsible use of the Internet", and "awareness of fraud, identity theft, cyber predators" while ethics is concerned with “cyber ethics”. Security in this instance however is for some reason used without the prefix ‘cyber’ (ibid.).

Further, this campaign shall draw upon previous public safety campaigns such as awareness of fire safety and seat belt safety. For these reasons, involving “celebrities”, the IT-generation, and “new types of media” to disperse the message seems appropriate (ibid.).

In conclusion, the cyberspace governance directed towards civil society deals with fostering docile subjects. And it may be a condition, for consent of hegemony to even be possible.

4.2.6. A Foreign Policy of Cyber Governance

Last of all, when it comes to foreign policy, some of the multilateral commitments of the contemporary administration are rendered partly evident. The CPR first of all states that the effort of securing cyberspace requires multilateral efforts (Cyberspace Policy Review 2009: 20). The modality of this claim is absolute. As stated by the CPR, this is an issue comprising three fields of governance: “territorial jurisdiction, sovereign responsibility, and use of force.” (ibid.). Since, by the conclusion of former chapters, this cannot be solved within the contours of the Nation; it is somehow vaguely demonstrated that it subscribes to a tendency towards a hegemonic formula.

First of all, the distinction between ‘territorial jurisdiction’, ‘sovereign responsibility’ and ‘the use of force’ deserves some elaboration. It might reasonably be seen in light of the contemporary global structure which have some notions of a post-Westphalian order with ‘universal norms’ of states as part of an international community (Etzioni 2006; Glanville 2011). For example, such as ‘sovereign responsibility’ having the communitarian meaning of the responsibility of states enshrined in norms within the International Community.

The approach proposed by the CPR highlights the importance of both multilateral and plurilateral engagements. The former indicated by the reference to “international bodies”, the International Telecommunications Union (ITU), and the International Organization of Standardization (ISO), and the United Nations. And the latter is expressed as commitments to “military allies and intelligence partners.” Especially within NATO (ibid.: 20). Other plurilateral organizations which address issues of cyberspace which is expressed as important platforms is the Council of Europe, the Group of Eight, the Asia-Pacific Economic

Cooperation forum, the Organization for Economic Cooperation and Development, and the Organization of American States.

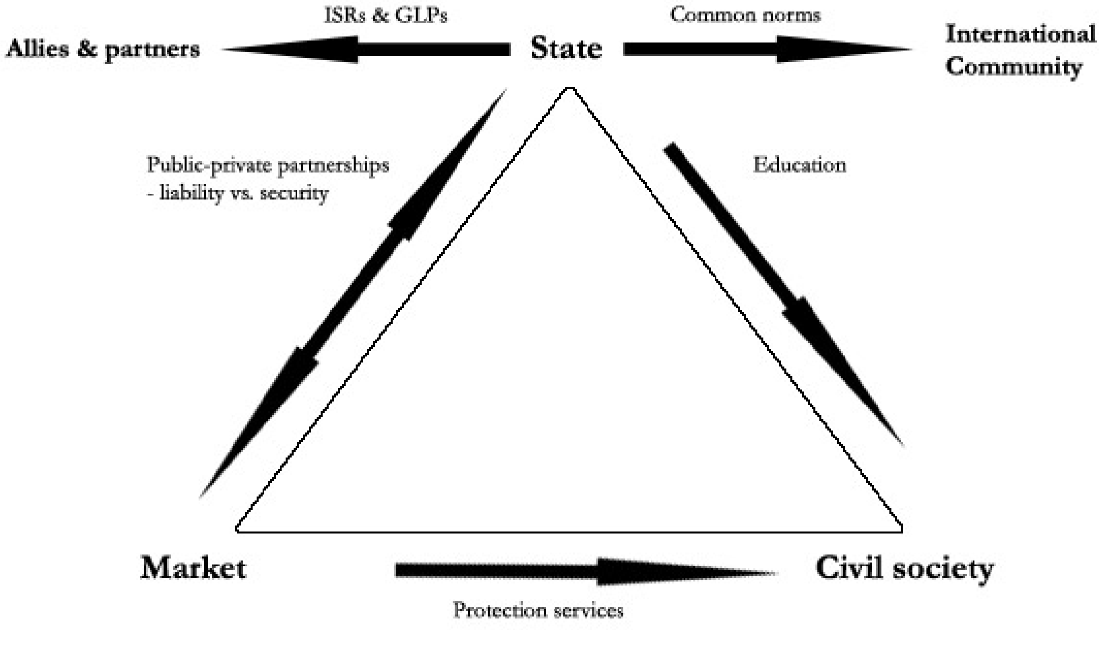
The CPR propose a "proactive engagement plan" for the coordination of "development, refinement, or reaffirmation of positions" to take into account interests of economics, national security, public safety and privacy (ibid.: 20). A concern expressed in the CPR is that the contemporary work conducted within the mentioned organizations has conflicting or overlapping scopes of practices, agreements and standards. The consequence of this is expressed as putting a "strain" on the capacity of the United States. Even though this heads slightly off-topic, this approach is by large in line with the 'assertive multilateralism' pursued by the Obama-administration.

This is concluded by some of the assumptions underlying this passage of the CPR. It is for example, inter alia stated with absolute modality that past experience "indicates the United States *will need to remain* engaged in a range of international activities." (my emphasis) (ibid.: 21). This might indicate that the importance of U.S. multilateral engagements is not a *modus operandi* of axiomatic significance. But that it is rather dependent on an assertive rationale for the purpose of preserving hegemony.

As was elaborated in the former section, the complexities of sovereign governance over cyberspace make private sector involvement prioritized. This is further highlighted in the proposed foreign policy of the CPR by reference to the private sector as an actor central to coordination and expansion of "international partnerships" (ibid.). This policy is concerned with international 'information sharing regimes' (ISRs) and 'government liability protections' (GLPs) that will facilitate efforts to help host countries of concerned global corporations to develop practices and standards in line with the United States. *Strategic* and *operational* collaborations are also included in this proposition. The definite meaning of this is unclear; although it is a plausible speculation that it entails efforts to make subject governments adopt a similar model of cyber governance as the United States (i.e. public-private partnerships of ISRs). These measures, however, create once another obstacle for the willingness of U.S. businesses to enter 'information sharing regimes', since they are reluctant towards having information shared with other countries or especially the International Community (ibid.: 28).

In conclusion, there is no ambition of acting in isolation in this regard, the United States is clearly eager to safeguard their position in multilateral engagements. As has been expressed before, this thesis argues that cyberspace viewed in the light of a 'global common' could pedagogically be compared to the importance of safeguarding maritime traffic on the high seas. It holds similar features as its function to the global capitalist system is concerned. Since the factor of time and space is collapsed in cyberspace, in comparison to a sea, it might even be regarded as even more critical to the operability of some economic functions. In summary, the most fundamental issue at hand is 'security' and 'resiliency', which by semantic relations are constituted as contrastive. 'Security' understood in reductive terms revolves around the capacity of enforcing boundaries in layers of spheres of protean liability in relation to degrees of protections and their perimeters, while 'resiliency' (cyberspace interoperability) is necessarily constrained by boundarizations. This compels for the importance of maintaining hegemony of cyberspace not for resiliency to suffer from competing models of governance. The figure below depicts the sum of the governance formula accounted for in this chapter.

Figure 1. *U.S. Cyber Governance*



4.3. Actors - The Agents of Cybersecurity

This section will outline the levels of analysis central to the study of *securitization*, which by virtue of its function, argued by this thesis; cannot be separated from the nature of governance. As regards the representation of referent objects, referent subjects, and functional actors in an emerging process of securitization, the findings of this thesis argues that in terms of the genre of the CPR, it cannot be convincingly argued that the CPR itself is an act of securitization. As is emphasized by Fairclough, genre is important for the interaction caused by a text (2003: 66ff). And since the CPR, in essence of its genre (proximate context), is probably not at the concern for most U.S. citizens, one could rather reckon that the outcome of the CPR after institutionalization within the political system is where the actual product of securitization will take potent form. The CPR is therefore rather a 'blueprint of securitization'. Nonetheless, the representation of referent subjects, referent objects, and functional actors in the CPR highlights important discursive constructions subject to this undertaking by the state.

4.3.1. The Construction of Referent Subjects & Referent Objects

The identification of referent subjects and objects was conducted by analysis of the construction of threats in the CPR. Although the CPR clearly states that it "remains a question unresolved" (Cyberspace Policy Review 2009: 28) as whether digital infrastructure not in the possession or property of the government should be protected and defended by the government, it nonetheless refer to the entities subject to the notion of security in the various elaborative passages, and indicates a classical instinctive will of the state thereof.

For example, "*The United States* <u>needs</u> a comprehensive framework to ensure coordinated response and recovery by *the government*, *the private sector*, and *our allies* to a significant *incident or threat*." (my emphasis) (ibid.: i). This sentence represent 'the United States' as the *referent object*, and 'the government', 'the private sector' and 'allies' as *referent subjects*, or even partly conflates the two into the referent subject. The term "needs" indicates strongest possible modality in the certainty of this claim. Elsewise, when the certainty is not as absolute, words such as "may need" is used instead. The identity of the threat is not represented, as is partly a general feature throughout the entire CPR.

But this picture have some depth to it, another referent object is for example represented in the next sentence:

> *The United States* needs to conduct a national dialogue on cybersecurity to develop more public awareness of the *threat and risks* and to ensure an integrated approach toward *the Nation's* need for *security* and the national commitment to *privacy rights* and *civil liberties* guaranteed by *the Constitution and law*." (my emphasis) (ibid.).

In this instance, "the United States" is represented as a *securitizing actor*, in need to take upon the quest of informing the general public on the threats facing the referent subject, "the Nation". The Constitution, or its concrete agent as enshrined in the Supreme Court, is designated as a *functional actor* in this regard. It is not represented as involved as an agent of national security but rather as an agent concerned with the core national values dependent upon national security. The CPR effectively constructs the notions of *security* and *liberty* as positively reciprocally conditioned. One is not possible without the other, and as such, this may have the purpose to diminish the tendency of discourse that security threatens liberty and vice versa. This seems to be a prerequisitional dichotomy for the discourse to hold together.

Another section of the CPR represents a similar image of threat: "cybersecurity risks pose some of the most serious *economic* and *national security* challenges of the 21st Century. […] a growing array of *state* and *non-state actors* are compromising, stealing, changing or destroying information that could cause critical disruptions to *U.S. systems*." (ibid.: iii). Contrary to the former section, this statement provides a much wider image. It indicates that the threat is mainly of economic and national security concerns, and makes a distinction between the identities of the threats. The variety of constellations is summed up in the table below.

Table 1. *Constellation of Security Referents*

Threats	**Referent object**	**The construction of threat**	**Referent subject**
'Nation-states'	The Nation, the United States	Undermine confidence, damage economic competitiveness and military technological advantage	The United States & Allies
'Criminals'	The Nation, digital infrastructure, privately owned infrastructure, the private sector	Undermine confidence	Private network operators
'International criminal groups'	U.S. citizens, commerce, critical infrastructure, government	Compromise, steal, change, or destroy information	the United States & Allies
'Domestic terrorists'	Privately owned infrastructure, the private sector	Physical intrusion or sabotage	Private network operators
'Terrorists'	U.S. citizens, commerce, infrastructure, government	Compromise, steal, change, or destroy information	the United States & Allies
'Malicious actors'	People, Industry, Global financial services	Affect competitiveness, degrade privacy and liberties protections, undermine national security, and cause general erosion of trust, or cripple society. Cause fraudulent transactions. Disrupt electric power. Compromise intellectual property, fraud, and identity theft	the United States & Allies, the Federal, State, local and tribal governments, the private sector

In sum, the CPR offers some indications on what kind of threats that is facing the United States or the Nation. The referent subject is the state and market, vocabulary differs between The United States and their allies, Federal, State, local and tribal governments, the private sector and private network operators. The referent objects is the Nation, the United States, U.S. citizens, people, the private sector, and digital infrastructure referred to in a myriad of different words. Functional actors are at the other hand not referred to very extensively; one mention is the Constitutional agents which were interpreted as law enforcement agencies and the court system. But as stated in the beginning of the section, this is the CPR vision for a blueprint of securitization rather than an act of the process itself.

4.4. Acts – A 'Blueprint of Securitization'

The analysis of *acts* within securitization theory is concerned, plainly speaking, with measures; the strategic use of symbols and instruments to engender specific modes of thoughts in the audience (See section 2.3.). In the particular case of the CPR, this comprised of the language used to present the narrative of cyberspace threat. This part may have been the most challenging in terms of interpretation. Since it is concerned with words used to facilitate mobilization, it is necessary to have a thorough understanding of American ideology and culture, as well as political traditions of domestic and foreign policy. What is not said is also of similar importance to what is actually said. This section outlines the two facets of these acts, *dispositifs* and *heuristic artifacts*, and how they are intimately connected.

4.4.1. The Dispositifs of Cyberspace Securitization

As when it comes to the *dispositifs* of securitization (measures), the CPR offers a very detailed prescription. All of the measures to secure cyberspace is collected in the "near-term action plan", consisting of ten imperatives of action (Cyberspace Policy Review 2009: 38).

The first measure [1] is to create a mechanism known as the "cybersecurity policy official" (CPO) for the coordination of U.S. cyber policies and activities (ibid.: 4-11). The next step [2] is to, by the imposition of this mechanism; prepare an updated national strategy to "secure the information and communications infrastructure." (ibid.). This is followed by [3] a designation of cybersecurity as a presidential priority, this also includes the creation of metrics to measure the performance of the adopted strategies. The fourth point [4] is concerned with the legitimacy of this practice, it entails the designation of a "privacy and civil liberties official to the NSC cyberspace directorate" (ibid.), which is under the direction of the CPO.

Next, the CPR suggests a [5] convocation of interagency mechanisms that is found appropriate under [2] to achieve coherence of policy, clarifying roles and responsibilities. All of these five initial points are reforms to be enacted within the state apparatus itself. The sixth point [6] on the other hand targets civil society in the initiation of a "national public awareness and education campaign to promote cybersecurity." (PAC) (ibid.: 13-15). Further, the seventh [7] is directed towards foreign policy and proposes development of government positions for an "international cybersecurity policy framework" as well as strengthening of international partnerships. The eighth point [8] touches upon the relation between government and market, and suggests a preparation of a "cybersecurity incident response plan" (IRP) by engaging in dialog to enhance public-private partnerships. All of the former is addressed at the domain of the cyberspace actual. The last two however, known as "game-changing" measures, engages the cyberspace real. It proposes [9] a research agenda to promote technologies that "have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure" (ibid.). And lastly, the CPR proposes [10] to build an "identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy enhancing technologies for the Nation." (ibid.). The use of language in this last point is quite astute, for it is in the very nature of identity management to rather deteriorate privacy; that is the whole point. All of these dispositifs, as well as their *legitimation*, *sphere of interaction*, and *type* (regulatory instrument or capacity tool) are assessed in the table below. (The CPR also lists a mid-term action plan, this however, was not identified as dispositifs of securitization but rather strategies of governance once securitization is successful). Further details are outlined in the next section.

Table 2. Dispositifs of securitization

Dispositifs	**Legitimation**	**Spheres of interaction**	**Type**
[1] Appoint CPO	Authorization/Moral evaluation	State [CPO ~ NSC-NEC]	**Capacity tool**
[2] Prepare national strategy	Rationalization	State [CPO ~ CNCI]	**Regulatory instrument**
[3] Designate cybersecurity priority	Authorization	State [CPO ~ the President]	**Capacity tool**
[4] Designate Privacy & Civil liberties officer to NSC	Moral evaluation	State [NSC]	**Capacity tool**
[5] Convene interagency mechanisms	Authorization	State	**Regulatory instrument**
[6] Initiate public awareness campaign	Mythopoesis	State ~ Civil society	**Regulatory instrument**
[7] Strengthen positions & partnerships	Rationalization	State ~ International Community	**RI/CT**
[8] Prepare CS incident response plan	Rationalization	State ~ Market	**RI/CT**
[9] Develop R&D strategies	Rationalization	State ~ Market	**Capacity tool**
[10] Build identity management vision & strategy	Rationalization	State ~ Civil society	**Capacity tool**

4.4.2. Heuristic Artifacts – Mobilizing Consent

Heuristic artifacts, as the symbols used to mobilize an audience (See section 2.3.), is to a great extent a question of addressing ideology. This part of the analysis will by systematical means try to locate some of the fundamental values connected to the words used to present the dispositifs in the CPR as outlined in the previous subsection of this chapter. To strengthen the interpretation I have also accounted for the heuristic artifacts in terms of legitimation (Fairclough 2003: 98) as indicated by the table in the former section.

First of all, the appointing of a CPO [1], the attainment of a national policy [2], and an elevation of presidential priority [3] is packaged within a frame of ensuring 'resiliency' and 'trustworthiness' for the support of "economic growth, civil liberties and privacy protections, national security, and the continued advancement of democratic institutions". This effectively resonates with 'what is at stake' (authorization, rationalization and moral evaluation). Interesting as it is, all of these 'goals' is not mentioned in other sections. To the contrary, mostly 'economic' and 'national security' issues are emphasized (Cyberspace Policy Review 2009: 7-9). It further put focus upon concepts such as 'anchoring leadership' in the 'White House' and employ a language suitable for indicating roles of coordination rather than 'rigid' modes of governance (authorization). This is definitely a hard case for interpretation, but it seems as if the heuristic artifacts deployed attempts to appeal to both a long-standing mythology of American legacy and at the same time to a sort of 'management discourse'.

On the first hand, there is the utterance of 'needs of the Nation', 'civil liberties', 'privacy rights', 'public safety',' national and economic security interests', which the CPO will seek to address (moral evaluation). It also refers to 'counterterrorism' or the far more interesting formulation of "countering terrorist use of the Internet" (ibid.: 8). This feature however, should not be over-exaggerated. On the other hand, the role of the CPO is to promote 'accountability', 'transparency', 'effective management', 'crisis management', 'flexibility and diversity', 'build trust' and engage in 'interagency coordination processes' by 'mission bridging' (rationalization). The function of the CPO is summed be the use of the word 'harmonize'. As such, the CPR does not engage in any 'hawkish' use of language. However, obvious as it is, the function of the CPO is to 'centralize' *operational* capabilities across agencies (horizontal centralization), guided by the *strategic* authority from above (vertical centralization) (legitimated by authorization).

‘What is at stake’, as has been accounted for above, returns throughout the passage in different guises. In one instance it is an “assured, reliable, secure, and resilient” digital infrastructure, in another it is an “assured, reliable secure and *survivable*” digital infrastructure, indicating a fear for its existence.

These heuristic artifacts referred to above also concern implementation of the [4] privacy and civil liberties official to the NSC cyberspace directorate, it draws upon words such as “signal transparency” and “build trust”. This is interesting, since if ‘signaling transparency’ is the purpose, in contradistinction to for example ‘upholding transparency’; then transparency is clearly about the production of legitimacy in ‘the eyes of the public’ and not transparency for the sake of transparency.

The doctrine of harmonization is also invoked to resonate with the need for interagency mechanisms [5]. This measure is captured by the term “mission bridging” (authorization) (ibid.: 7).

Secondly, concerning educating the general public [6] the CPR could not plead deeper to the American ideology than it does, starting with: “The Nation is at a crossroads”. It then goes on to refer to the ‘undergoing’ of a ‘revolution’ of digital technology and the ‘dual challenge’ of promoting “innovation, open interconnectivity, economic prosperity, free trade, and freedom while also ensuring public safety, security, civil liberties, and privacy.” (mythopoesis/moral evaluation). Once again, the language is not very ‘hawkish’, one could easily think of replacing the last clause of the sentence with ensuring ‘national security, military technological advantage, and so on’. Because that is what it is partly about, the research program proposed states clearly that its goal is to create a workforce suitable for these matters.

It further goes on to quote the President, a quote of him urging America to prepare their children for global competition. And draws a comparison to the contemporary challenge with that following the launch of the Sputnik satellite in 1957. Words such as “the information age economy” are used to contextualize the current needs of technological education (mythopoesis). This effectively becomes a point for assembling all parts of the Nation by mention of the critical role the technological programs have for “Hispanic, and historically Black colleges” and the integration of state and market by opening up mobility for professionals to achieve a beneficial “cross-fertilization”. For a state dominated by men, ‘fertility’ is likely a fine phrase.

The other part of this dispositif, which concerns “risk awareness”, is in the words of the CPR in need of an “effective communication strategy” (rationalization). Once again a sound word that could exhilaratingly just as well be replaced by ‘propaganda’. This strategy aims to create “digital safety, ethics, and security” and shall “promote responsible use of the internet”. “The threat” is referred to in singular, and to further the persuasion the CPR mentions previous similar campaign such as Smokey Bear on fire safety and the Click It or Ticket campaign for seat belt safety. This is, as the CPR states, “Imperative to the Nation’s health, security and prosperity in the 21st Century.” (ibid.: 13-15).

Further, the justification for the need for assertive multilateral action [7] begins by delivering a decisive blow against isolationism, arguing that “The federal government cannot succeed […] if it works in isolation” (rationalization) (ibid.: 17). This need for cooperation also encompasses the relation between government and private sector [8]. Both of the claims are expressed in strongest possible modality. The CPR uses words such as “the global challenge of securing cyberspace”, by development of “global standards”, “best practices” and an “environment of trust” to maintain “stable and effective Internet governance”, “transparency” and “public confidence” (rationalization) (ibid. 17-19).

As for the “game-changing” research programs [9], the CPR raises the narrative of “integrated vision” between the government, the private sector, and “other stakeholders” (rationalization). This is the only section in the CPR where the word “stakeholders” is used. It emphasizes the need for creation of “a family” for the coordination of objectives. By the entreating reference to the private sector as a “steward of the public interest” (ibid.: 32). And lastly, the dispositif of establishing identity management mechanisms [10] resonates to its subjects by highlighting that the clues people use to establish trust in daily interaction is absent in the case of virtual interaction (rationalization). The modality of the CPR is absolute in its claim that cybersecurity “cannot” be improved without the improvement of authentication, but less certain about the potential of identity management mechanisms to improve ‘privacy’ (it “has the potential”) (ibid.: 33). Ironically, this seems to indicate some honesty to the matter.

In conclusion, the heuristic artifacts used to resonate with the audience should certainly be seen in light of its genre. And by virtue of its genre they have the character of a combination between mythological notions of American historical legacy (mythopoesis and moral evaluation) and governmental management discourse that may resonate with the ear of policy-makers and politicians (authorization, but especially rationalization).

5. Conclusion

It is clear that answering the questions whether it is possible to identify a process of securitization within U.S. cyberspace policy, and how ‘governance’ is represented in U.S. cyberspace policy; does not fall short of ambiguities.

Any concluding remark will therefore remain humble to the complex reality of interpretation and hermeneutics within the discipline of social science. But, in a critical realist fashion, complexity does not mean that ‘anything goes’. Some consistent tendencies are definitely visible. The contextual meaning of ‘cybersecurity’ can be said to encompass the dimensions of military, economic, political, societal, technological, and maybe even ecological security. The term is understood as a domain of security, not a dimension.

The *distal context* for the need of cybersecurity is envisaged as a condition for the hegemony of the United States. It shall be emphasized that, according to discourse, excessive cybersecurity would be detrimental to maintaining hegemony, and would undoubtedly lead the United States into a rule by dominance. Thereof, the administration rather pursues hegemony in the precise Gramscian sense of the word. It seeks the consent of its subjects. Governing cyberspace according to the CPR is in great abstraction, as I stated, an art of ‘governing without smothering’.

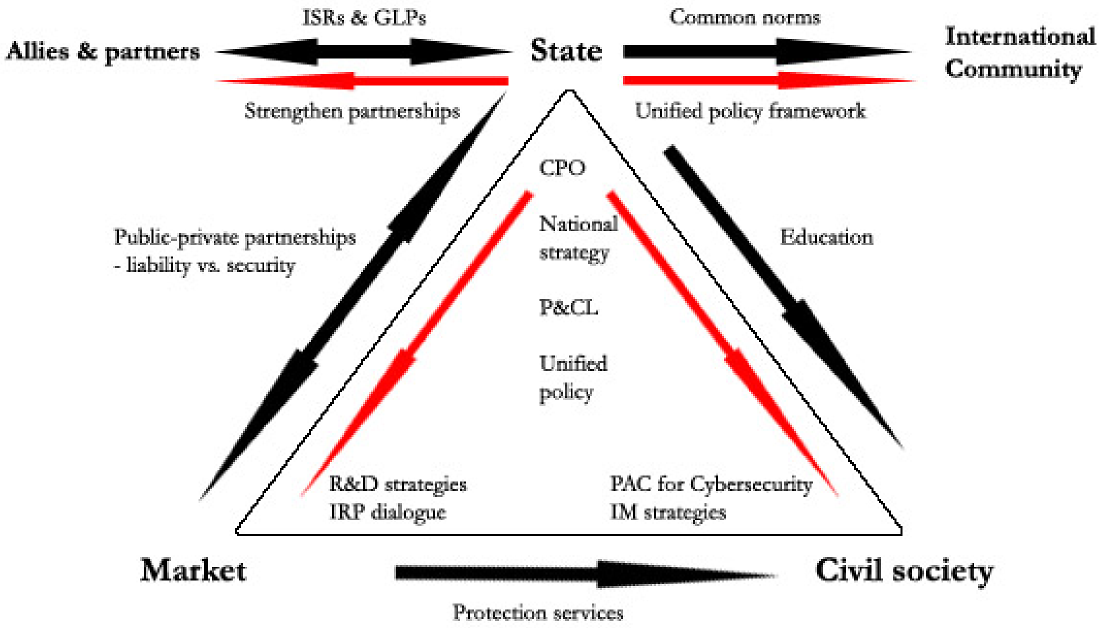
This principle applies to all spheres of society, but differently. Governing the state is concerned with the production of coherent policy. This is also the imperative of engaging in multilateral or plurilateral efforts with other states. Governing the market (both national and global) regards a corporativist model. And governing civil society is directed at the production of a popular discourse of security, serving the needs of the hegemonic interest; that of acquiring ‘resiliency’ and ‘security’ in the realm of cyberspace.

I argue as was envisaged before embarking upon this analysis that this formula of governance elaborated above, cannot be separated from the process of securitization. But whether a process of securitization has taken place or not, cannot be concluded by this thesis. I do conclude however, that the Cyberspace Policy Review is a ‘blueprint of securitization’. Securitization should neither be viewed in absolutes, as something that had occurred or not; but as a continuous process of securitization or de-securitization by the production of discourse. Right now the former seems to be more present than the latter. Regarding the constellation of agents: referent objects and subjects could not be clearly defined, although a tendency was evident. Both state and market can be regarded as referent subjects *and* objects. Civil society is definitely a referent object, although unclear to what extent.

Acts on the other hand, as in the dispositifs (measures), could be identified in their potential form. The heuristic artifacts used to resonate with the political establishment which shall adopt this policy, could also be assessed. They are primarily legitimated by rationalization.

Finally, it nonetheless seems as if the basic criteria of securitization (that something is declared as threatened, and that measure is taken for its protection) are met, although the circle is not yet sealed. I thus conclude, that cyberspace is in the process of being securitized in the U.S. context, but it cannot be concluded that it will succeed, and the formula of governance outlined in the thesis, be implemented. The sum of this formula is captured by the figure below.

Figure 2. Securitization of U.S. Cyberspace



The read arrows in the figure are meant to depict the sphere of interaction for the dispositifs of securitization. While the black ones are the essence of the governmental relations of power in the realm of cyberspace. What in first instance could be read as a hegemonic model of cyber governance could not be effectively divorced from the specter of security in any aspect. Since the potential dispositifs of cyberspace securitization can be identified in the CPR I therefore conclude that hegemony in this particular case is mainly revolving around the process of seeking the acceptance from the subjects of governance for 'the need' of security.

6. Discussion

Carl Schmitt once wrote that "sovereign is he who decides on the exception" (2005: 5). I think great relevance still lies within this claim, but 'he' himself resides in the multitude. A Gramscian approach to the analysis of governance and securitization as has been utilized in this thesis expose this phenomenon quite clairvoyantly. It is obvious that the state cannot be solely regarded in the reductionist sense but must encompass the entire interaction operating in the hegemonic interest. Such as the role of education in securitization, and how the sometimes called 'state-market nexus' even influences what is to be regarded as the sovereign responsibility of the state.

One of the main insights in conducting this study is that, what some securitization theorists like to call "exceptional measures"; is not too exceptional at all. The economic-security nexus has according to some, always strongly influenced security policy in the United States. Securitization in this sense must be viewed in strictly constructivist terms, and following Felix Ciută (2009), cannot be both a 'speech act' and 'surviving'. That would make 'security' and 'securitization' into interchangeable terms. Securitization must rather be a process by which something is declared a matter of security regardless of any real existential threat underlying such act. Further, although my analysis does not account of it, it is obvious how actors participating in the production of discourse in the CPR can partake as a securitizing actor without the interest of creating the predicament for exceptional political measures. The cyber protection systems industry for example, does clearly want to convince an audience of the need for cybersecurity, but is equally reluctant towards exceptional measures of governments.

Discourse of hegemonic governance viewed within the frame of securitization also has some rather peculiar character. It is not as if the subjects of governance are taken into account in governmental discourse at face value, rather, securitization is a *condition* for them to enter into the hegemonic order. Governmental discourse has it that people cannot value security, and ultimately, to be governed; if they do not 'know' what is at stake. This makes sense; why else would security seem inevitably to be a rather normative concept, in a relative way. As Stefano Guzzini (2011) has argued, it is not unduly to designate securitization the status of a causal mechanism that holds contingent liabilities toward social objects, having the potential to be actualized under certain circumstances. Thus, I finally take it to be the case that *hegemony* in its very striving for consent of subalterns is more dependent and consanguineous to securitization than other conformations of governance.

Bibliography

Abrahamsson, H. (2008). *Det gyllene tillfället: Teori och strategi för global rättvisa*. Stockholm: Leopard Förlag.

Acharya, A. (2007). "State Sovereignty After 9/11: Disorganised Hypocrisy". *Political Studies*, vol. 55, pp. 274-296.

Appadurai, A. (2006). *Fear of Small Numbers*. Durham: Duke University Press.

Bajaj, K. (2010). *The Cybersecurity Agenda: Mobilizing for International Action*. New York: The EastWest Institute.

Bachrach, P. & Baratz, M. (1962). "The two faces of power". *American Political Science Review*, vol. 56, no. 4, pp. 947-952.

Balzacq, T. (2005). "The Three Faces of Securitization: Political Agency, Audience and Context". *European Journal of International Relations*, vol. 11, no. 2, pp. 171-201.

Balzacq, T. (2011). *Securitization Theory – How security problems emerge and dissolve*. London & New York: Routledge.

Barkin, J. S. (2010). *Realist Constructivism: Rethinking International Relations Theory*. Cambridge: Cambridge University Press.

Bartelson, J. (1995). *A Genealogy of Sovereignty*. Cambridge: Cambridge University Press.

Bhaskar, R. (1975). *A Realist Theory of Science*. London & New York: Verso Books.

Biersteker, T. & Weber, C. (1996). *State Sovereignty as a Social Construct*. Cambridge: Cambridge University Press.

Blommaert, J. & Bulcaen, C. (2000). "Critical Discourse Analysis". *Annual Review of Anthropology*, vol. 29, pp. 447-466.

Bromley, S. (2003). "Reflections on Empire, Imperialism and United States Hegemony". *Historical Materialism*, vol. 12, no. 3, pp. 17-68.

Bull, H. (1977). *The anarchical society: A study of order in world politics*. New York: Columbia University Press.

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

Campbell, D. (1998). *Writing Security – United States Foreign Policy and the Politics of Identity*, Revised Edition. Manchester: Manchester University Press.

Castells, M. (2001). *Internetgalaxen: Reflektioner om internet, ekonomi, och samhälle*. Göteborg: Daidalos.

Choucri, N. & Goldsmith, D. (2012). “Lost in cyberspace: Harnessing the Internet, international relations, and global security”. *Bulletin of the Atomic Scientists*, vol. 68, no. 2, pp. 70-77.

Ciută, F. (2009). “Security and the problem of context: a hermeneutical critique of securitization theory”. *Review of International Studies*, vol. 35, no. 1, pp. 301-326.

Clark, I. (2009). “Bringing hegemony back in: the United States and international order”. *International Affairs*, vol. 85, no. 1, pp. 23-36.

Clark, I. (2011). “China and the United States: a succession of hegemonies?”. *International Affairs*, vol. 87, no. 1, pp. 13-28.

Cornish, P. & Hughes R. & Livingstone, D. (2009). *Cyberspace and the National Security of the United Kingdom: Threats and Responses*. London: Chatham House.

Cox, M. (2010). “Whatever Happened to American Decline? International Relations and the New Unites States Hegemony”. *New Political Economy*, vol. 6, no. 3, pp. 311-340.

Cox, R. W. (1983). “Gramsci, Hegemony and International Relations: An Essay in Method”. *Millenium – Journal of International Studies*, vol. 12. no. 2, pp. 162-175.

Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure, Washington DC, 2009.

Dahl, R. (1961). *Who Governs: Democracy and Power in an American City*. New Haven: Yale UP.

Deibert, R. J. & Rohozinsky, R. (2010). “Risking Security: Policies and Paradoxes of Cyberspace Security”. *International Political Sociology*, vol. 4, pp. 15-32.

Derrida, J. (1979). *Spurs Nietzsche’s Styles / Éperons Les Styles de Nietzsche*. Chicago & London: The University of Chicago Press.

Mullis, K. (2009). “Playing Chicken with Bird Flu: ‘Viral Sovereignty,’ the Right to Exploit Natural Genetic Resources, and the Potential Human Rights Ramifications”. *American University International Law Review*, vol. 24, no. 5, pp. 943-967.

Esaiasson, P. & Gilljam, M. & Oscarsson, H. & Wägnerud. L. (2007). *Metodpraktikan: Konsten att studera, samhälle, individ och marknad*. Tredje upplagan. Stockholm: Norsteds Juridik.

Etzioni, A. (2005). *Sovereignty as Responsibility*. Elsevier Limited, Foreign Policy Research Institute, winter 2006.

Fairclough, N. (2003). *Analysing Discourse: Textual analysis for social research*. London & New York: Routledge.

Glanville, L. (2010). “The antecedents of ‘sovereignty as responsibility’”. *European Journal of International Relations*, 2011, vol. 17, no. 2, pp. 233-255.

Gramsci, A (2010 [1971]). *Selections from the Prison Notebooks*. New York: International Publishers.

Gilje, N. & Grimen, H. (2007). *Samhällsvetenskapernas förutsättningar*. Göteborg: Daidalos.

Goffman, E. (2009 [1959]). *Jaget och maskerna – En studie i vardagslivets dramatik*. Norstedts.

Guzzini, S. (2011). ”Securitization as a causal mechanism”. *Security Dialogue*, vol. 42, no. 4-5, pp. 329-341.

Hacking, I. (2000). *Social konstruktion av vad?* Stockholm: Thales.

Halpin, E. & Trevorrow, P. & Webb, D. & Wright, S. (2006). *Cyberwar, Netwar and the Revolution in Military Affairs*. New York: Palgrave MacMillan.

Hannum, H. (1996). *Autonomy, Sovereignty, and Self-Determination – The Accommodation of Conflicting Rights*. Revised Edition. Philadelphia: University of Pennsylvania Press.

Heickerö, R. (2012). *Internets mörka sidor: Om cyberhot och informationskrigföring*. Stockholm: Atlantis.

Hettne, B. (2009). *Från Pax Romana till Pax Americana – Europa och världsordningen*. Stockholm: Santérus förlag.

Higham, P. (2005). Keeping it Real: A Critique of Postmodern Theories of Cyberspace. In López, J. & Potter, G. (2005). *After Postmodernism: An Introduction to Critical Realism*. Second Edition. London & New York: Continuum.

Hobson, J. M. (2002). What’s at stake in ‘bringing historical sociology back into international relations’? Transcending ‘chronofetishism’ and ‘tempocentrism’ in international relations. In: Hobden, S. & Hobson, J. M. (2002). *Historical Sociology of International Relations*. Cambridge: Cambridge University Press.

Hughes, R. (2010). “A treaty for cyberspace”. *International Affairs*, vol. 86, no. 2, pp. 523f.

Ikuenobe, P. (2003). “Optimizing Reasonableness, Critical Thinking, and Cyberspace”. *Educational Philosophy and Theory*, vol. 35, no. 4, pp. 407-424.

Joyner, C. & Lotrionte, C. (2001). “Information Warfare as International Coercion: Elements of a Legal Framework”. *EJIL*, vol. 12, no. 5, pp. 825-865.

Keohane, R. (2000). “Sovereignty in International Society”. In D. Held & A. McGrew (eds), *The Global Transformation Reader – An Introduction to the Globalization Debate*. Oxford: Blackwell Publishers.

Knake, R. K. (2010). *Internet Governance in an Age of Cyber Insecurity*. Council on Foreign Relations, Council Special Report No. 56.

Koepsell, D. R. (2000). *The Ontology of Cyberspace: Philosophy, Law, and the Future of Intellectual Property*. Chicago: Open Court Press.

Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton NJ: Princeton University Press.

Kurki, M. (2007). "Critical Realism and Causal Analysis in International Relations". *Millennium - Journal of International Studies*, vol. 35, pp. 361f.

Laclau, E. & Mouffe, C. (2001). *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso Books.

Lessig, L. (2002). "Code and Other Laws of Cyberspace". *Radical Philosophy Review*, vol. 5 no. 1-2, pp. 204-206.

Lessig L. (2006). *Code*. Cambridge: Basic Books.

Lewis, J. A. (2010). "Cyberwarfare and its impact on international security". *Unoda Occasional Papers*, no. 19.

López, J. & Potter, G. (2005). *After Postmodernism: An Introduction to Critical Realism*. Second Edition. London & New York: Continuum.

Lukes, S. (2005 [1974]). *Power: A Radical View*. Basingstoke: Palgrave Macmillan.

McEvoy Manjikian, M. (2010). "From global village to virtual battlespace: the colonizing of the internet and the extension of realpolitik". *International Studies Quarterly*, vol. 54, no. 2, pp. 381-401.

McNally, M. & Schwarzmantel, J. (2009). *Gramsci and Global Politics – Hegemony and resistance*. New York: Routledge

Michelfelder, D. P. (2000). "Our moral condition in cyberspace". *Ethics and Information Technology*, vol. 2, pp. 147-152.

Moolakkattu, J. S. (2009). "Robert W. Cox and Critical Theory of International Relations". *International Studies*, vol. 46, no. 4, pp. 439-456.

Nagorski, A. (2010). *Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway*. New York: The EastWest Institute.

Ned Lebow, R. & Kelly, R. (2001). "Thucydides and hegemony: Athens and the United States". *Review of International Studies*, vol. 27, pp. 593-609.

Nye, J. S. Jr. (2010). *Cyber Power*. Cambridge: Harvard Kennedy School.

Ong, A. (2000). “Graduated Sovereignty in South-East Asia”. *Theory, Culture & Society*, vol. 17, no. 4, pp. 55-75.

Patomäki, H. & Wight, C. (2000). “After Postpositivism? The Promises of Critical Realism”. *International Studies Quarterly*, vol. 44, pp. 213-237.

Phillips, N. (2007). “The Limits of ‘Securitization’: Power, Politics and Process in US Foreign Economic Policy”. *Government and Opposition*, vol. 42, no. 2, pp. 158-189.

Philpott, D. (2001). *Revolutions in Sovereignty: How Ideas Shaped Modern International Relations*. Princeton NJ: Princeton University Press.

Saull, R. (2012). “Rethinking Hegemony: Uneven Development, Historical Blocs, and the World Economic Crisis”. *International Studies Quarterly*, vol. 56, pp. 323-338.

Sayer, A. (2000). *Realism and Social Science*. London: Sage Publications.

Sayer, A. (2010). *Method in Social Science: A realist approach*. Revised Second Edition. London & New York: Routledge.

Schmitt, C. (2005 [1922]). *Political Theology: Four Chapters on the Concept of Sovereignty*. Chicago & London: The University of Chicago Press.

Segal, A. (2011). *Cyberspace Governance: The Next Step*. Council on Foreign Relations, Policy Innovation Memorandum No. 2.

Spinello, R. 2002. *Regulating Cyberspace: The Policies and Technologies of Control.* Westport: Quorum Books.

Sprague, J. (2005). *Feminist Methodologies for Critical Researchers: Bridging Differences*. Walnut Creek: Altamira Press.

Tavani, H. T. (2001). “The state of computer ethics as a philosophical field of inquiry: Some contemporary perspectives, future projections, and current resources”. *Ethics and Information Technology*, vol. 3, pp. 97-108.

Young, G. & Whitty, M. (2011). “Progressive embodiment within cyberspace: Considering the psychological impact of the supermorphic persona”. *Philosophical Psychology*, vol. 24, no. 4, pp. 537-560.

Zhao, S. (2004). “Consociated Contemporaries as an Emergent Realm of the Lifeworld: Extending Schutz´s Phenomenological Analysis to Cyberspace”. *Human Studies*, vol. 27, pp. 91-105

Žižek, S. (1996). “Cyberspace, or the Virtuality of the Real”. *Journal of the centre for Freudian analysis and research*, vol. 7.

Annex

1) The identity of the participants in the assessment of the CPR, differentiated and sorted by societal sphere, type of operation, field of operation, and number of printed issues in the assessment. (Based upon estimation)

Identity of participants	*Sphere*	*Type*	*Field*	*No.*
Center for National Security Studies	Civil societal	Research & advocacy org.	National	1
Center for Progressive Regulation	Civil societal	Non-profit research org.	National	1
Electronic Frontier Foundation	Civil societal	Donor-supported rights protection org.	Global	1
Accenture	Corporate	Management consultant	Global	1
Bell Aliant	Corporate	Internet-provider	Regional	2
American Chemistry Council	Corporate	Business member org.	Global	2
Booz Allen Hamilton	Corporate	Management & tech consultant	National	2
Business Executives for National Security	Corporate	Nonpartisan business org.	National	1
Oracle Corporation	Corporate	Computer tech corporation	Global	1
Economist Intelligence Unit	Corporate	Business research org.	Global	1
Forrester	Corporate	Research & advisory company	Global	1
Crucial Point LLC	Corporate	National security tech company	Global	2
Harris Interactive	Corporate	Market research company	Global	1
Information Technology Information Sharing and Analysis Center	Corporate	Non-profit security specialist org.	Global	1
Internet Corporation for Assigned Names and Numbers	Corporate	Non-profit domain name provider	Global	1
Internet Security Alliance	Corporate	Non-profit collaboration org.	National	10
Core Security Technologies	Corporate	Cybersecurity company	Global	2
National Cyber Security Alliance and Symantec	Corporate	Cybersecurity company	Global	1
Wurldtech Labs	Corporate	Cybersecurity company	Global	1
SANS Institute	Corporate	Computer safety training company	Global	2
TechAmerica	Corporate	Tech industry association	National	1
U.S. Chamber of Commerce	Corporate	Business federation	National	1
Board of Governors of the Federal Reserve System	Corporate/Gov.	Central bank	National	1
Center for Democracy and Technology	Corporate/Gov.	Non-profit organization	National	2
Computer Research Association	Corporate/Gov.	Association of academia	National	1

Capital Markets Research	Governmental	Academia	National	1
Congressional Research Service	Governmental	Public policy research org.	National	2
Defense Advanced Research Projects Agency	Governmental	Government agency	National	1
Department of Defense	Governmental	Government department	National	2
Department of Health & Human Services	Governmental	Government department	National	1
Department of Treasury	Governmental	Government department	National	4
Educational Technology, Policy, Research and Outreach	Governmental	Tech education org.	National	1
Financial Services Information Sharing and Analysis Center	Governmental	Business forum	National	1
National Association of State Chief Information Officers	Governmental	State-gov collaboration org.	National	1
National Coordination Office for Networking and Information Technology Research and Development	Governmental	Government agency	National	1
National Cyber Forensics & Training Alliance and Cyber Initiative & Resource Fusion Unit	Governmental	Government agency	National	1
National Science and Technology Council	Governmental	Government agency	National	1
National Science Foundation	Governmental	Independent gov-agency	National	4
National Security Telecommunications Advisory Committee	Governmental	Government advisory board	National	1
Networking and Information Technology Research and Development Program	Governmental	Federal research program	National	1
Office of the Director of National Intelligence	Governmental	Government office	National	1
United States Government Accountability Office	Governmental	Investigative public org.	National	1
United States Secret Service	Governmental	Government agency	National	1
National Cyber Security Alliance	Corporate/ Governmental	Public/private partnership org.	National	1
William Jackson	Individual	Scholar	National	1
Kevin R. Pickney	Individual	Scholar	National	1
Harry D. Jr Raduege	Individual	Scholar	National	2
Eugene H. Spafford & Kenneth p. Birman	Individual	Scholar	National	1
Stephen Spoonamore & Ronald L. Krutz	Individual	Scholar	National	1
Paul Trevithick & William Coleman	Individual	Scholar	National	2
Jaikumar Vijayan	Individual	Scholar	National	1
Cato Institute	Non-	Libertarian think tank	Regional	1

	govermental			
Information Systems Audit and Control Association	Non-govermental	IT-gov specialist org.	Global	1
SRI International	Non-govermental	Non-profit science inst.	Global	1
Carnegie Mellon CyLab	Private	Private university	Global	1
Carnegie Mellon University	Private	Private university	Global	1
Massachusetts Institute of Technology	Private	Private university	National	2
Intelligence and National Security Alliance	Private	Non-profit nonpartisan security org.	National	3
Georgetown University	Private	Private university	National	1
Markle Foundation	Private	Philanthropy org.	National	1
Cornell University	Private	Private university	National	1
Indiana University	Public	Public university	National	1
Purdue University	Public	Public university	National	1
George Mason University	Public	Public university	National	1
University of Minnesota	Public	Public university	National	1
University of California	Public	Public university	National	1
National Research Council	Public	Public research org.	National	1
United States Congress	Public	Parliament (hearings)	National	2
United States House of Representatives	Public	Parliament (hearings)	National	17
United States Senate	Public	Parliament (hearings)	National	5

2) Analytical scheme 1. Modalities

Prevalent modalities	**Deontic**	**Epistemic**
High	must, needs to	will (require/ensure), would (require/ensure), has (not), are/is/does (not), that (require)
Median	should	has (the potential), risks,
Low	may (need)	may (require), can, could (require)

3) Coding scheme 1. Semantic relations

[PARATAXIS] (Clauses are grammatically equal)

[HYPOTAXIS] (One clause is subordinate to the other)

{CAUSAL} (**REASON**, **CONSEQUENCE**, **PURPOSE**)

{CONDITIONAL} (Conjunction makes latter clause conditional on the former)

{TEMPORAL} (Conjunction is temporal)

{ADDITIVE} (Conjunction is adding between the clauses)

{ELABORATIVE} (Conjunction is elaborating, by exemplification)

{CONTRASTIVE/CONCESSIVE} (Conjunction is contrasting the clauses)

One might wonder what the significance of these might be. From my experience they are only useful in concert with exchange types described on the next page. If for example the text expresses an epistemic assertion, you can differentiate whether that assertion is for example *conditional* on another assertion, or if assertion itself hinges on a demand which is not epistemic. It is also helpful to identify discursive causalities, what the authors' holds for causal liability among their procedures, and so on.

However, identifying these conjunctions is often a severe struggle. It is not always the case that they are marked by explicit markers. I am not prestigious enough to try to uphold a façade of academic excellence in conducting my interpretation by use of this coding procedure. Actually, it was quite painful. Thus, I would in fact not suggest any student of International Relations to use this method if not for having read at least a semester of linguistic studies. I have not studied linguistics myself, and this meant: a lot of sleepless nights during the coding procedure. It took me some weeks to get on track and without a very decisive attitude it could possibly lead to intellectual break-down. Therefore, if I knew what I know now before embarking on this study, I would read some linguistics.

4) Coding scheme 2. Exchange types

	Truth (Epistemic)	**Obligation (Deontic)**

High
E: Certainly
D: Required
	{EPISTEMIC S-ASSERTED}
	Statement (S) is asserted. Such as ‘cyberspace is endangered’
	{EPISTEMIC S-DENIED}
	Statement (S) is denied. ‘Cyberspace is *not* endangered’
		{DEONTIC D-PRESCRIBED}
		Demand (D) is absolute. ‘Do that’. No subject
		{DEONTIC D-PROSCRIBED}
		Negative absolute demand (D). ‘Do *not* do that’. No subject
		{DEONTIC O-UNDERTAKEN}
		Offer (O) is undertaken. ‘The government will do that’
		{DEONTIC O-DENIED}
		Offer (O) is denied. ‘The government will *not* do that’

Median
E: Probably
D: Supposed
	{EPISTEMIC S-MODALIZED}
	Statement (S) is ‘modalized’. Such as ‘that may happen’.
	{EPISTEMIC Q-POSITIVE}
	Positive question (Q). Such as ‘is that the case?’
	{EPISTEMIC Q-NEGATIVE}
	Negative question (Q). ‘Is that *not* the case?’
		{DEONTIC D-MODALIZED}
		Demand (D) is modalized. Such as ‘the government should do that’

Low **E: Possibly** **D: Allowed**	**{EPISTEMIC Q-MODALIZED}** Question (Q) with low degree of modality. ‘Could that happen?’ Very rare in the CPR	**{DEONTIC O-MODALIZED}** Demand is an offer (O) with low degree of modality (modalized), such as ‘the government may do that’

I must confess that I am not a hundred percent sure that this coding system of mine would be endorsed by Fairclough from which I have derived these exchange types (2003: 167-171). I would be humble to all contestations. It may for example seem strange that modalized deontic offers is located at a low degree while deontic modalized demands are located at median level. However, I do think that an imperative of ‘subject should’ is a stronger case than ‘subject may’. Some of these exchange types is also furthermost used in dialogue and is therefore not identified at a single instance in the CPR. Below is an example of how these codes was used in the process of collecting data from the CPR.

5) Example of coding procedure:

“The national dialogue on cybersecurity must **{EPISTEMIC S-ASSERTED}** ***begin today.*** The government, working with industry, should **{DEONTIC D-MODALIZED}** explain this challenge **[PARATAXIS]** and **{ADDITIVE}** discuss what the Nation can do to **{CAUSAL-PURPOSE}** solve problems in a way **[PARATAXIS]** that **{CONDITIONAL}** the American people can appreciate the need **{EPISTEMIC S-ASSERTED}** for action. People cannot **{EPISTEMIC S-ASSERTED}** value security **[HYPOTAXIS]** without **{CONDITIONAL}** first understanding how much is at risk **{EPISTEMIC S-ASSERTED}**.”(Legitimation: **Rationalization)**

When some of my friends and associate students within IR or Political Sciences saw me conducting this procedure, their spontaneous reaction was to start worry that insanity was impending. I did not blame them, for what is it that you are actually doing while conducting this coding procedure? At the beginning I was not sure myself, and by large surmised to the diagnosis of insanity. But after a while I started to realize its potential. It simply de-politicizes the text in a very useful manner. After a while you cannot see all of the value-laden concepts of ‘Nation’, ‘terrorism’, ‘freedom’ and so on, but rather starts to look upon the text as a structure. You start to see a clear distinction between claims of truth and claims of obligation, and you can interpret in a less biased manner. You can conclude that, well, here we have, for example, a causal purpose that is epistemic in nature. That seems strange, because how is a purpose connected to knowledge if not normative? And so on. However, when analyzing heuristic artifacts and so on, then you have to disembark slightly from this attitude. But, nonetheless, the coding procedure gave me a lot of confidence in the reliability of my conclusions. The coding procedure definitely guides interpretation in a manner that enables you to identify things that would not be apparent from just ‘reading’ the text.

Now, returning to the example above, why did I conclude that these two sentences legitimate action by *rationalization* and not *authorization*? Well, simply because we have one deontic offer of obligation, but four epistemic assertions of truth. Epistemic assertions outnumber deontic offers. And as such, rationalization is more prevalent than authorization. However, the code is blind to mythopoesis for example; therefore, you have to engage in a certain extent of hermeneutic activity that does not concern the coding.

Analytical scheme 2. Semantic relations (example of significant contrastive[s])

Resilience	**Security**
innovation, open interconnectivity, economic prosperity, free trade, freedom	public safety, security, civil liberties, privacy

6) Analytical scheme 3. Examples of legitimation of ante-natal procedures in the CPR.[2]

Legitimation	Authorization	Rationalization	Moral evaluation	Mythopoesis
Dispositifs of securitization	It is the fundamental responsibility of our government to address strategic vulnerabilities	People cannot value security without first understanding how much is at risk.	The United States faces the dual challenge of maintaining an environment that promotes innovation, open interconnectivity, economic prosperity, free trade, and freedom while also ensuring public safety, security, civil liberties, and privacy.	Similar to the period after the launch of the Sputnik satellite in October, 1957, the United States is in a global race that depends on mathematics and science skills.
Public-private partnerships	During a significant cyber incident, as with other major national incidents, only the White House has the authority to coordinate the wide array of capabilities and authorities involved in incident response.	The Federal government has the responsibility to protect and defend the country, and all levels of government have the responsibility to ensure the safety and wellbeing of citizens. The private sector, however, designs, builds, owns, and operates most of the digital infrastructures that support government and private users alike.		ensure the Nation's continued ability to compete in the information age economy . Only through such partnerships will the United States be able to enhance cybersecurity and reap the full benefits of the digital revolution.
Centralization of operational capabilities	Leadership should be elevated and strongly anchored within the White House to provide direction, coordinate action, and achieve results.	The United States should harness the full benefits of technology to address national economic needs and national security requirements.		

[2] As is emphasized by Fairclough (2003: 98ff), legitimation of ante-natal procedures are often explicitly motivated. Most common at the contemporary time is legitimation by reference to utility: rationalization. This holds for the CPR as well. However, as he also emphasize, most of them overlap in considerable ways, this is just an example of how some sentences of motivations was interpreted.