Ontological Security: State Identity and Self-Image in the Digital Age

Robert James Ralston

Thesis submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Master of Arts
In
Political Science

Priya Dixit, Chair
Scott Nelson
Laura Zanotti

9 May 2014
Blacksburg, Virginia

Keywords: Ontological Security, Cyberspace, Power, United States, Self-Image, State Identity

Ontological Security: State Identity and Self-Image in the Digital Age

Robert James Ralston

ABSTRACT

The driving argument of this thesis is that states, particularly the United States, are vulnerable in cyberspace for reasons that go beyond the material vulnerabilities that present studies on state insecurity in cyberspace focus on. This vulnerability in cyberspace is an ontological insecurity. Ontological insecurity reveals itself in the contradictions in official state discourse regarding cyberspace. State security of self—preserving and maintaining the seemingly concrete and consistent nature of what a state is about, how the state is understood in relation to other states, and how the state comes to understand itself through its own conceptions of self-identity—is challenged by cyberspace as a vehicle for massive amounts of information and challenges to state identity in relation to the state's behavior in cyberspace. Therefore, state identity and self-image are challenged in relation to cyberspace in two ways: first, through the vehicle that is cyberspace, and, second, through the practices that the state adopts to secure cyberspace and its broader security aims. The language that states, in this case the United States, use in order to justify surveillance practices and to impose meaning to cyberspace ultimately leads to projections of power that attempt to reinforce state strength and legitimacy vis-à-vis cyberspace, but these attempts fall short; contradictions arise in state discourse, and weaknesses are highlighted through these contradictions. Cyberspace, then, is an ontological as well as physical security threat to states.

For Katie

Table of Contents

Chapter 1: Introduction

Addressing the Senate Select Committee on Intelligence on the 12th of March, 2013, James Clapper, the United States' Director of National Intelligence, argued that 'cyber-' is now at the top of the United States' transnational threat list. Clapper argued: "Attacks, which might involve cyber and financial weapons, can be deniable and unattributable […] Destruction can be invisible, latent and progressive."[1] There is a growing sentiment, expressed by Clapper during the committee meeting, that "[t]he intelligence community must continue to promote collaboration among experts in every field, from the political and social sciences to natural sciences, medicine, military issues and space." Meanwhile, Nazli Choucri (2012: 3) notes that cyberspace has moved from an issue of 'low politics' to a matter of interest in 'high politics.' Cyberpolitics and cybersecurity, it seems, has reached a critical moment in the study of international politics and national security.

Current accounts of cyberwar, cybersecurity, and cyberpolitics stress the importance of bringing analysis to bear, or for analysis to catch up with, the burgeoning interdependent and permeable nature of cyberspace. Cyber policy and analysis lag behind the ever-connecting and ever-expanding networks that permeate national boundaries and jurisdictions. Care must be taken in order to keep analysis "on the ground," so to speak: there are very real physical—as well as intangible—aspects and features of cyberspace. Indeed, it is easy to think of cyberspace as a "cloud" creating a "borderless world" in which states have absolutely no power whatsoever to control access, censor information, etc. These social-scientific fantasies should be reined in, but

[1]See the Press Release by the Department of Defense here: http://www.defense.gov/news/newsarticle.aspx?id=119500 (Accessed 1 May 2014).

not dismissed; policy, public opinion, and the like often deal in these terms, and thus have a certain validity, or at the very least, an analyzable quality.

Something is missing in current accounts of cybersecurity, particularly in the study of international politics. While there can be no doubt that state security, or insecurity, with regards to cyberspace take on physical and informational aspects—cyber security and information security, respectively—cyberspace poses another different kind of insecurity for states: ontological insecurity. This thesis seeks to explain state ontological insecurity in the digital age through an examination of official state discourse about cyberspace and the leaks by Edward Snowden by the Obama Administration. The main research question that guides this thesis is: *how does the state conceptualize its own identity and security in relation to cyberspace?* A series of questions follow: *how is state intrusion into cyberspace justified and legitimated?* and, *how are contradictions to state self-image and identity mediated?*

The driving argument of this thesis is that states, particularly the United States, are vulnerable in cyberspace for reasons that go beyond the material vulnerabilities that present studies on state insecurity in cyberspace focus on. This vulnerability in cyberspace is an ontological insecurity. Ontological insecurity reveals itself in the contradictions in official state discourse regarding cyberspace. In particular, the leaks by Edward Snowden about the National Security Administration's surveillance program(s) present an aesthetic irruption of state self-image that can be examined comparatively; how was cyberspace talked about prior to and after these allegations of widespread surveillance? The characteristics of cyberspace that provide accelerated opportunities in the digital age unsettle the state, and the need for a consistent self-identity and self-image can lead the state to ultimately adopt practices that may run counter to self-image, or that is in line with self-image while being strategically nonsensical.

Thus, this thesis is ultimately about state identity and self-image in relation to cyberspace, particularly after the NSA disclosures made by Edward Snowden. State security of self—preserving and maintaining the seemingly concrete and consistent nature of what a state is about, how the state is understood in relation to other states, and how the state comes to understand itself through its own conceptions of self-identity—is challenged by cyberspace as a vehicle for massive amounts of information and challenges to state identity in relation to the state's behavior in cyberspace. Therefore, state identity and self-image are challenged in relation to cyberspace in two ways: first, through the vehicle that is cyberspace, and, second, through the practices that the state adopts to secure cyberspace and its broader security aims. The language that states, in this case the United States, use in order to justify surveillance practices and to impose meaning to cyberspace ultimately leads to projections of power that attempt to reinforce state strength and legitimacy vis-à-vis cyberspace, but these attempts fall short; contradictions arise in state discourse, and weaknesses are highlighted through these contradictions. Cyberspace, then, is an ontological as well as physical security threat to states, because cyberspace is seemingly uncontrollable, and offers a vehicle from which pressures can be put on the state in relation to its self-image and identity. The NSA leaks proved just that—suddenly the United States was cast in opposition to the very values it purports to uphold: an Orwellian surveillance state, practices of surveillance violating Constitutional rights, etc. Edward Snowden, in this analysis, represents a pressure, or counterpower, to state attempts to define and secure cyberspace. Snowden highlights only one example of cyberspace as a vehicle for challenges to state self-image and identity; there are countless attempts at such pressure from a global cyber audience including other states, non-governmental actors, and the likes of WikiLeaks.

The importance of this study is twofold, politically and in terms of the field of international relations. First, politically, ontological insecurity reinterprets the motivations and rhetoric of state actors, in this case against the backdrop of cyberspace. State agents, in this account, seek to solidify or reinforce state identity in the wake of challenges that arise from cyberspace of state self-identity. Second, in terms of the field of international relations, the concept of ontological security challenges a traditional assumption of IR: that states interact in an anarchic system based on each state's individual material, territorial, and physical survival. Rather, this thesis extends an enhanced understanding of state security in the digital age: state physical security is important—and cyberspace by its very interdependent and permeable nature certainly causes physical insecurity—but the identity of the state is constantly under duress in cyberspace. What the state is, or should be, is constantly articulated in a new domain of interaction for citizens of the state, and a global audience. This phenomenon draws the state into attempts to reinforce its own self-image globally, through official state agents, who ultimately reveal contradictions in the practices of the state, further drawing criticism by way of challenges to state self identity. Thus, the relationship of the state vis-à-vis other states is not entirely about security-seeking actors acting in an anarchic system of international relations; the relationship of the state vis-à-vis other states is also about identity-seeking and identity-reinforcing actors acting in a new digital age that constantly draws attention upon the actions and discourses of the state. This thesis extends one such case: the leaks by former National Security Administration (NSA) contractor Edward Snowden and the response that the leaks brought about.

What is at stake as cyberspace becomes an issue of high politics, and as states attempt to address fundamental security concerns arising from cyberspace, be they physical insecurities or other types of insecurity? The state, and the agents who narrate about the state, frame cyberspace

in a way that attempts to "cover up" "cracks" in the discourse that arise by way of contradictions of self-image. States justify intrusion into cyberspace in the name of stability and an idealized self-image. This, in other venues, can prove violent and costly, such as Thatcher's 'resilience' in dealing with the Argentinean invasion of the Falkland Islands, all in the name of 'empire.' In cyber venues, the United States in particular has had to justify state intrusion into a new kind of space; void of routinized responses to "traditional" threats, discourse must reshape or reconfigure the self-image of the state in order to combat the contradictions inherent in state intrusion into cyberspace. Such intrusion is justified by the inherent usefulness of the Internet for the state to gather information and in the state's desire, in a post-9/11 world, to preemptively stop new kinds of perceived security threats.

Self-image and identity are important in the context of cyberspace because cyberspace provides a vehicle from which to present alternatives to self-image and identity in a space that is accessible to the constitutive members of a nation-state, as well as a global audience. These alternative depictions that can run counter to self-image and contradictory to state identity are not easily controlled by way of state censorship, and are countless, which leaves addressing them all virtually impossible. Thus, cyberspace provides a multitude of reflections upon state self-image that leave the state insecure and incapable of defending, rhetorically, all of the opposing narratives that arise. Other factors, including the speed of which these counter-images are shared and distributed in cyberspace makes states vulnerable. Chapter three provides a rationale as to why the United States in particular is vulnerable in this regard.

What is cyberspace? Cyberspace carries with it inherent political meanings (Cavelty 2013: 107). The term was originally coined by William Gibson, a cyber-punk novelist, and was imported into the policy domain first by John Perry Barlow, a self-proclaimed cyber-libertarian

(ibid.). This conceptualization by Barlow forms the origin of cyberspace as a new place, and thus a space that "allows different notions of control and domination over virtual lands" (ibid.). At its core, "cyber" encompasses three broad elements: technical, informational, and human aspects of cyberspace and subsequently cyber security and cyberwarfare (Kramer 2009: 4). According to the 2003 *National Strategy to Secure Cyberspace*, "cyberspace" is defined as a "nervous system—the control system of the country … composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructure to work" (National Strategy to Secure Cyberspace 2003: vii). However, this definition of cyberspace is not an exhaustive one; cyberspace, as it is presented in this thesis, is, to a certain extent, what states make of it. Therefore, while cyberspace has infrastructural, informational, and interactive qualities and dynamics, what is important here is how states come to understand cyberspace vis-à-vis their own security.

This thesis is split into five chapters that first draw together the theoretical lens through which the state discourse is to be examined (ontological security, power as aesthetic), then applies this analytical lens to a specific case, the United States' various attempts to define cyberspace and the U.S. reaction to widespread allegations of invasive surveillance in cyberspace. The second chapter provides an overview of ontological security, and an examination of aesthetic power. The notion of power as aesthetic and the concept of ontological security are linked through an understanding of the importance of state-self image; aesthetic power is the state's ability to act upon its own self-image, while ontological insecurity harkens back to state (in)security of self. The third chapter briefly outlines the use of discourse analysis in the study of international relations. Language, is an extension of state power to shape what the United States thinks cyberspace *should be*, as well as to recreate, reinforce, and stabilize

state-image. This language is examined in the fourth chapter, which empirically examines official discourse from the Obama administration, pre- and post- Snowden disclosures, to highlight contradictions to self-image that arise in state discourse regarding cyberspace as an application of the theory of ontological security in international relations. In chapter four, the analysis will focus on various representations of state self-image and self-identity that arise in the discourse of cyberspace, as well as in visual representations of self-identity and self-image that occurred during the South by Southwest Conference (SXSW) in March of 2014. Here, official discourse is examined to demonstrate ways language is used as an expression and extension of state power: narratives of American exceptionalism, preserving American values in a new arena of interaction, ahistorical references to legitimate widespread surveillance, and deflections of responsibility. All of these narrative deployments are part of U.S. self-image and identity—an identity and image that constantly needs to be reinforced through language. Finally, the fifth chapter concludes by offering a broad overview of the main arguments in the thesis, as well as future directions for research.

Chapter 2: Ontological Security and Power as Aesthetic

i. Introduction

Physical security concerns dominate realist accounts of security in world politics (Mitzen 2006: 342). In cyber contexts, popular accounts of cyber war (Clarke 2010) and cybersecurity (Singer 2014) focus on cyber threats in terms of espionage, critical infrastructure defense, and how cyber wars can translate into "traditional" combat domains. Nazli Choucri (2012: 153) notes that the analysis of cyberpolitics, in cases such as cyber terrorism, cyber crime, and cyber security are "already characterized by already defined political spaces in which actors, stakes, contentions, and potential outcomes are delineated, at least at the start—even if the identity of all the actors is not known."

This chapter elaborates on an alternative conception of security and power that goes beyond a conception of security as solely based on survival and power based solely on material/physical security and strength. While traditional notions of material interest, security, and power are important in the structure and dynamics of international politics, this chapter focuses on ontological security in international relations. Cyberspace challenges state security of self. First, this chapter will advance a notion of ontological security, which presents state behavior in terms of the ways in which a state seeks to preserve its identity. Second, this chapter describes the aesthetic nature of power. States face ontological insecurity in their relationship with cyberspace. State understanding is based on a conception of security and power that is "stuck" in material ways of thinking. Aesthetic power, the ability to maintain and, if necessary, reconfigure, self-image is key in terms of the ontological security of the state and how such a

construction of self-image is engaged by citizens (Steele 2010: 2). This argument is critical to an understanding of how states come to understand cyberspace, and how states respond to challenges that come from cyberspace, which will be studied in the next chapter. For instance, surveillance programs, like the massive NSA surveillance program, *may* secure the physical interests of the state, but pose a larger threat to states in the form of presenting an unwanted self-image.

ii. Ontological Security

The term "ontological security" was initially coined by R. D. Laing, a psychiatrist, who focused on the ontologically secure individual (Zarakol 2010: 6). The term was then adapted by the sociologist Anthony Giddens[2], who defined ontological security as "the confidence that most human beings have in the continuity of their self-identity and in the constancy of the surrounding social and material environments of action" (Zarakol 2010: 6). In terms of the state, ontological security means having a consistent sense of what the state represents by way of values, history, and the like. Ontological insecurity, then, arises for the state when the state's sense of identity is challenged through interrogations of state behavior and state narratives in relation to state identity. Steele (2008) summarizes ontological security in security studies: "Nation states seek ontological security because they want to maintain *consistent self-concepts,* and the "self" of states is constituted and maintained through a narrative which gives life to routinised foreign policy actions."[3] Consistency is important for the state in terms of its ontological security; cyberspace produces challenges to state self-concepts, and, thus, presents a new challenge to state identity through the constant relaying of various representations of the state, projected back and in relation to the narratives and practices that make up the state.

[2] Referenced in Zarakol (2010); original quote: Giddens, *The Consequences of Modernity* (1990)
[3] Emphasis in original; Narrative, to Steele, is methodologically important in the study of ontological security

The preoccupation and assumption that states seek only physical security, Mitzen (2006: 364) argues, constrains international relations theory by failing to explain why states may seek or continue conflict, for example, at the expense of physical security. The argument that unquestioned assumptions can blind IR scholarship is an important point here. State behavior in relation to cyberspace, I will argue, contains elements of material and physical security concerns, and rightly so. However, scholarship can analyze states in relation to cyberspace one step further: understanding how cyberspace, as an interconnected, fluid, and permeable space,[4] poses challenges to state identity and power is equally, if not more, instructive for IR scholarship. Ontological insecurity is concealed in state discourse about cyberspace. In contrast, states can explicitly leverage concerns related to physical insecurity to provide justification for intrusion into cyberspace, even though such intrusions can seemingly run counter to the self-image the state wishes to maintain in world politics.

Ontological security in international relations shifts the analytical focus away from understanding security solely as a state's physical need for survival. Jennifer Mitzen (2006) and Brent Steele (2008) target an underlying assumption in international relations theory: "…that nation-states are primarily concerned with their survival" (Steele 2008: 1). Preoccupation with survival as the primary motivation for state behavior fails to capture the ways in which states operate that are social and representational in nature. Ontological security is security of the self (Mitzen 2006: 341). Steele (2008: 2-3) suggests that ontological security is more important to states than physical security, "…because its [ontological security] fulfillment affirms a state's self-identity (i.e. it affirms not only its physical existence but primarily how a state sees itself and secondarily how it wants to be seen by others)." For Steele, ontological security is a prerequisite

[4] Choucri (2012: 4)

for physical security. Mitzen (2006: 342) further suggests that ontological security "…refers to the need to experience oneself as a whole, continuous person in time—as being rather than constantly changing—in order to realize a sense of agency." The notion that ontological security is fulfilled by experiencing the self as whole and continuous in time is challenged by the very nature of cyberspace as a 'space' that permeates national boundaries and jurisdictions, that disseminates information in a manner which is difficult to control, and a space that presents a plethora of different depictions and representations of the state.

Routine is central to an understanding of ontological security. Routine in security studies, from the perspective of the state, is so important that states may forgo other values in an effort to maintain identity through routine. Routine, in this context, is about achieving ontological security by attempting to eliminate uncertainty vis-à-vis other important others in international relations (ibid.: 342). According to Mitzen (2006: 346), routines, unlike rational action, repress reflection in favor of the act of repression itself: "…this suppression is the source of their security-generating power. By giving actors automatic responses to stimuli, routines pacify the cognitive environment, bounding the arena of deliberative choice." Realists, Mitzen (2006: 354) argues, tend to place the blame for various pathologies of state behavior on actors inside of individual states operating in the anarchic system of international relations. Ontological security, on the other hand, places some explanation in the space between states, in the inter-state routines that states use to ensure ontological security (Mitzen 2006: 354). Routines are so important to state behavior, Mitzen argues, because routines "…that perpetuate physical insecurity can provide ontological security, states can become attached to physically dangerous relationships and be unable, or unwilling, to learn their way out" (2006: 354). Thus, routine,

through the lens of ontological security, can provide powerful explanatory power for seemingly pathological state behavior, which can include behavior that runs counter to state self-image.

State mediation of the uncertainty and threat generated by cyberspace can be understood in terms of the complicated nature of cyberspace as a *seemingly* deterittorialized 'space.' State routine, regardless of whether it perpetuates insecurity or security, is dominated by an understanding of interaction that is inter-state rather than inter-space. In other words, cyberspace presents a new kind of domain of interaction for states, a domain that perpetuates physical insecurity (in the way of very real and often unknown threats such as hacking, viruses, denial of service (DOS) attacks, etc.) and ontological insecurity (in the way of an uncertain and constantly shifting self-image). For example, the U.S. domination of sea, air, land, and space hinges on a conception of power and security that is based on material strength and physical dominance. Cyberspace is often described as an operational space (Kuehl 2009, 29). Similar to the other operational domains of land, sea, air, and space, cyberspace is painted as a bounded space in which national security actors can operate, as well as business and private enterprise. Cyberspace is now often referred to as the "fifth domain" of warfare ("The Economist" 2010). In terms of routine, this characterization of cyberspace reduces the significant differences between cyberspace and the domains of air, sea, land, and space that cyberspace is often now associated with. These differences range from broad theoretical issues regarding the nature of warfare (including alternative conceptions of violence), security, and capability in cyberspace to issues of internet governance, be they grounded in the physical infrastructure of cyberspace or in the information and interaction that takes place on the "content layer" of cyberspace. Absent of self-reflexivity, states have routinized responses to cyberspace, and other actors in cyberspace, that are grounded in routines that are more suitable for different domains of warfare, or simply

different domains of interaction. For example, the manner in which the British Ministry of Defense formulates and defends the creation of a new 'cyber task force' normalizes cyberspace as just another operational domain. Phillip Hammond, the Secretary of State for Defense, remarked:

> People think of military as land, sea and air. We long ago recognised [sic] a fourth domain - space. Now there's a fifth - cyber. […] You deter people by having an offensive capability. We will build in Britain a cyber strike capability so we can strike back in cyber space against enemies who attack us, putting cyber alongside land, sea, air and space as a mainstream military activity. ("BBC" 2013)

What is at stake in a routinized response to cyberspace? The stakes go beyond semantics; state response to cyber threats justify state practices in cyberspace, and ultimately seek to define what the role of cyberspace is vis-à-vis the state. Further, responses like Mr. Hammond's posture the state in relation to other states in cyberspace. These dynamics will be further explored in Chapter 3 by examining similar kinds of statements made by U.S. President Barack Obama regarding the United States' role in cyberspace and in confronting the leaks made by former NSA contractor Edward Snowden.

Ontological security is not without its critics. In terms of international relations scholarship, the arguments made for ontological security confront their own sets of issues, and according to Zarakol (2010: 6), run into their own versions of the agent-structure problem.[5] Ontological security in international relations goes beyond the premise that states are solely concerned with physical security.

Another critique is that ontological security presupposes that the state is like a person: ontological security is about the "self" of a state, but who is the state? Is this problematic? Mitzen (2006), Wendt (2004), and Steele (2006) offer justification for personification of the

[5] This split will be examined later in the chapter

state.[6] In an effort to counter critiques, or to offer justification, of ontological security, Jennifer Mitzen offers three defenses of ontological security. First, Mitzen argues that the notion that states are driven by physical security assumes that states have 'bodies' (2006: 351). This is equally as problematic to Mitzen as the notion that states have selves, in the case of ontological security: "Thus, the real issue here is not physical versus ontological security, but state personhood more generally" (2006: 352). The notion of state personhood is vital to an understanding of physical security, ontological security, and aesthetic power. Steele (2010: 3) notes: "…because state agents 'narrate' about the nation-state, they create potential Selves that the nation-state seeks to realize through its policies." The state as a "body" that has a "self" is crucial to this analysis. On the one hand, material threats from cyberspace threaten physical security, the "body." Furthermore, the notion of integrated networks and cyberspace as the "pulse" of the nation makes the threats that come from cyberspace seem more systemic and dangerous.[7] Narration by state agents is critical to an understanding not only of how states conceptualize threats to physical security, but how the self of the state is created in the first place.

Mitzen's second rationale of ontological security is that states are beholden to the individuals that make up a group identity, and thus states seek ontological security on the basis of their constitutive members (Mitzen 2006: 352). Routine here is again important; inter-societal routines "…help maintain identity coherence for each group, which in turn provides individuals with a measure of ontological security" (Mitzen 2006: 352). Cyberspace is often touted as a space that diminishes geographically and culturally-contingent interactions and connects,

[6] Alexander Wendt (2004) seeks to lay a philosophical groundwork for understanding why states are personified in international relations.

[7] For instance, the 2012 James Bond (007) film *Skyfall* portrays the United Kingdom as a completely integrated, digital, nation-state that is susceptible to the most egregious of physical attacks

virtually, groups of people from around the globe who have shared interests. How does cyberspace facilitate identity coherence on the basis of factors outside of the state's control? Finally, Mitzen points to how ontological security, in its micro-foundational assumption, explains macro-level patterns in international relations theory (2006: 352). States, as corporate actors, according to Mitzen, are made up of individual decision-makers, but these decision-makers behave in seemingly consistent ways (2006: 352).[8] Ontological security provides an explanation from the "top-down" to understand why the behaviors of individual decision-makers maintain consistency over time: states seek ontological security (Mitzen 2006: 353).

Beyond critiques of ontological security more generally, Zarakol (2010: 6) notes that there are two distinct "wells" in the deployment of the concept of ontological security in international relations. The tension that arises in the scholarship regarding ontological security is similar to the differences between Laing and Giddens, according to Zarakol. What is the origin of ontological insecurity? Does ontological insecurity arise from the interactions of states? Or, does it arise from the state's own uncertainty about its identity? The basis for chapter three is that ontological security seems to arise from the state's own uncertainty about its identity.

Scholars who have employed the concept of ontological security have done so with various approaches. While Mitzen (2006) utilizes Giddens' approach to ontological security—emphasizing the role of interaction in generating the ontological insecurity of states—Steele (2008: 58) argues that Mitzen overstates the role of interaction, and argues that the Self of the state generates the state's understanding of its environment, and thus, shapes it. Further, Steele (2008: 58-59) argues that Jennifer Mitzen misses the role of narrative in shaping the self-identity process: "Other scholars working on ontological security centralize the role of narrative in the

[8] Mitzen makes reference to Jervis (1976) and Larson (1997); different personalities and generations of leadership, these studies concluded, were beholden to macro-level rationalities (2006: 345).

self-identity process, suggesting that by organizing history in a particular fashion narrative constructs a salient group self-identity."[9] In terms of Mitzen's argument that states are dependent upon the social world, and make meanings from it, Steele (2008: 59) argues:

> I would agree with Mitzen that an agent must make sense of the social world to ensure ontological security. But this does not mean that this agent is "dependent" upon the social world, in that (1) the screening of "relevant" elements of that social world is in part constituted by an agent's sense of Self – in short, how an agent "makes sense" of those elements – is in part also dependent upon an agent's updating of information.

The difference between Mitzen (2006) and Steele (2008)'s arguments hinge on two sites of emphasis. First, as Zarakol (2010: 7) argues, the emphasis on either the agent or the structure, and, second, methodological emphasis; while Mitzen focuses on the study of interaction, Steele focuses on narrative.[10] There are middle grounds, however, between Mitzen and Steele;[11] Zarakol (2010) and Kinvall (2004) suggest alternative approaches to ontological security. Kinvall (2004: 748-749) argues that security can be understood as a 'thick signifier' that "highlights the intersubjective ordering of relations—that is, how individuals define themselves in relation to others according to their structural basis of power. This implies that individuals experience different levels of security in relation to their own and others' perceptions of the structural power position they are currently in." Kinnvall (2004: 749) goes on to argue that an increase in ontological insecurity causes an increased attempt to securitize subjectivity. That is, as ontological insecurity increases, attempts to search for one stable identity intensify (ibid.). Zarakol (2010) examines the denial of Turkish and Japanese historical crimes in an effort to examine, in a sense, whether Mitzen or Steele is more accurate in their analysis of ontological security: are identity pressures on states endogenous or exogenous? According to Zarakol (2010:

[9] Steele notes Kinnvall (2004) here

[10] The role of narrative in the study of ontological security will be examined in the next chapter in terms of methodology and case selection

[11] This does not suggest that Mitzen and Steele are on some sort of spectrum, where they are the polar endpoints

19), both Mitzen and Steele are *partly* right, but have a crucial omission in their analyses: "the uneven expansion of international society or the effect this expansion had on the identity of outsider states who were incorporated into the system at a later date." In other words, the cases used by Mitzen and Steele, the EU and Belgium/U.S. respectively, are inherently Western-centric examples that do not take into consideration 'other' states that must compare themselves to the West and seem to have to react to the West rather than to their respective selves (Zarakol 2010: 20).

In sum, ontological security, or ontological insecurity, is about the (in)security of the self of the state. In the study of international relations, ontological security is about constructing and maintaining the stability of the self of the state. Going forward, ontological security will be examined through the lens of discourse, in a vein similar to Steele (2008)'s work. However, there is a second element to the dynamic of state insecurity in cyberspace that must first be examined, and that is power—particularly the conception of power as aesthetic, which is inextricably linked to ontological security.

iii. Power as Aesthetic

Power is often characterized in international relations in terms of the material strength of nation-states. Distinctions are made between "hard power," military and economic coercion, and "soft power," cooperation and persuasion. In the study of international relations, nation-states, particularly powerful ones, are understood in terms of their ability and authority to maintain control of time and space (Steele 2010: 1). Barnett and Duvall (2005:39) argue that the study of international relations is primarily focused on one specific type of power: "an actor controlling another to do what it would not otherwise do." This, in Barnett and Duvall's view, is insufficient; no single view or definition of power, the authors argue, can capture what power

ultimately is in international relations (2005: 67). Rather, power can take many forms, and can be interrelated (ibid.: 67). Barnett and Duvall (2005: 48) categorize four different types of power in their taxonomy: compulsory, institutional, structural, and productive. Barnett and Duvall (2005: 42) offer a general definition of power as "the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate. The general concept of power that we employ is restricted to the production of particular kinds of effects, namely those on the capacities of actors to determine the conditions of their existence." This general concept of power is markedly different than that the authors argue dominates the field of international relations, and leaves room for alternative conceptions of power.

Power, according to Steele (2010: 15), can be understood in terms of "a centralized body's internal capacity to perceive its ability to operate upon its own self-image, as well as influence others and determine outcomes." Thus, power is not *solely* based upon a state's ability to make another actor do what it would otherwise not, to pose material threats to other states, global influence; power is about the state's recognition that it can use and recreate its own self-image. Hillary Clinton's *21st Century Statecraft* initiative for 'forging U.S. digital diplomacy' utilizes the internet to send out clear, and consistent, messages from ambassadors and other State Department figures.[12] Thus, cyberspace is not always a vehicle for criticizing the state; cyberspace can be used as a tool by the state in an effort to secure its self-image. However, the natures of 'trending' topics on Twitter, for instance, make such digital diplomatic efforts often risky. For example, seemingly innocuous social media posts can quickly devolve into critiques of state policy, or shine light on contradictions that are found within these digital diplomatic posts.

[12]See a description of 21st Century Statecraft here: https://blogs.state.gov/stories/2012/01/27/21st-century-statecraft-forging-us-digital-diplomacy (Accessed 1 May 2014).

States, much like people, engage in a series of aesthetic practices. Steele (2010: 3-5) equates the aesthetic practice of getting ready in the morning with how states continually engage in aesthetic practices. The purpose of getting ready in the morning is twofold. First, getting ready in the morning functions to make us appear slightly differently to others (Steele 2010: 3). Makeup, for instance, may make one appear to have a slightly different complexion; it is a practice of aesthetic management. Second, one assumes that getting ready in the morning makes an individual more admirable, or closer to an ideal that is set by the individual; the teenager who loves skateboarding, for instance, may aim for an aesthetic that differs quite differently from the businessperson getting ready for a busy day at the office. However, one important distinction, in terms of this aesthetic remains; unlike the teenager in the bathroom getting ready in the morning to re-create an image, states recreate and "get ready" out in the open through global information and the constant gaze of the world (Steele 2010: 5). The credibility of the state hinges not only on maintaining a sense of credibility in the face of the "other," but also maintaining a continual demonstration of power in order to fight off an internal feminine other, according to Weldes, who uses the Cuban Missile Crisis as an example of the conflict the United States has with the feminine other (1999:46).[13] However, as Steele (2010: 16) notes: "In an attempt to 'project strength,' these leadership narratives instead generated perpetual insecurity." Projections of strength ultimately focus attention on perceived weakness: the Ministry of Defense's declaration about its new cyber task force, on the surface, seems to solidify the United Kingdom's capability in cyberspace, but it also shines light on physical vulnerabilities in terms of cyber infrastructure that the state recognizes as needing to be secured.

[13] Cited in Steele (2010: 16)

Power, as aesthetic, has many dimensions. Steele (2010) outlines three "strata" of aesthetic power: psychological, imaginative, and rhythmic. The psychological stratum of aesthetic power ultimately leads to an inverse relationship: the more coercion deployed by centralized power is met with a decline in influence from the psychological stratum (Steele 2010: 29). The imaginative stratum of aesthetic power is particularly important in understanding the aesthetic of power surrounding state behavior in cyberspace. Steele (2010: 31) draws upon Lacan's theory of the mirror stage in development and extends Lacan's thought to how states view themselves in terms of imaginary power, "which interprets through the lens of Self the meaning of external events, each action that occurs "out there" *must* say something about the Self."[14] For instance, the United Kingdom's announcement of a cyber task force *must* say something about a declining relationship between the United States, cyber threats as they relate to the United States, etc. Thus, there is narcissism in imaginative power (Steele 2010: 31). Moreover, this mirror image of the Self that is reflected back upon the Self in imaginative power creates a vulnerability: "…it cannot predict which images of the Self will emerge, since it is looking everywhere for evidence of self-gratification and is bound to let down (down from the idealized Self)" (Steele 2010: 31). Unable to predict, and with any precedent, what images of the Self will emerge, states are left particularly insecure in cyberspace. Beyond the concerns that states face regarding hackers, electric power outages, etc., states are left ontologically insecure in cyberspace. Disruptions to a state's self-identity are just as vital to remedy as a state's physical security (Steele 2008: 2). Cyberspace is a reflection of the images of infinite, idiosyncratic, others.

[14] Emphasis in original

The rhythmic stratum of aesthetic power is about synchronization, which are coordinated movements in state agencies that respond when a crisis occurs (Steele 2010: 36). According to Steele, "..the Self of a body of power is constituted through routines that entail structures—structures that work back upon the agent by providing meaning to the latter's existence" (2010: 36). In terms of ontological security, this rhythmic stratum of aesthetic power is similar to the need of a state to have routine (Steele 2010: 37):

> The general scenario scales up an aesthetic construction of power's subjectivity with the rhythmic, seen through routinized movements of the body, and a narrator who imbues these movements with an ambiguous but compelling meaning for action, important for identity. The rhythmic stratum co-constitutes the psychological, as these routines provide us not only an anchor of ontological security of the Self but also emotionally satisfying narratives of what the Self is and what it means in time and space.

But what happens when the aesthetic construction of centralized power is de-aestheticized? Counterpower, a micropressure, seeks to challenge or rupture the aesthetic image (Steele 2010: 2). According to Steele (2010: 2), this de-aestheticization often is followed by a reaction by centralized power that is quick and sometimes violent.

Much has been written on counterpower and its relationship to technology. In a widely cited work on communication, power, and counterpower, Castells (2007), defines power and counterpower in structural terms. Castells (2007: 239) understands power in the traditional form that Barnett and Duvall (2005) critique. Similarly, Castells (2007: 239) views counterpower as a capacity to resist. Castells (2007: 258) seeks to understand the shift towards a network society and the rise of counterpower: "I am extending this analytical perspective to the historical dynamics of counter-power, as new forms of social change and alternative politics emerge, by using the opportunity offered by new horizontal communication networks of the digital age that is the technical and organizational infrastructure that is specific of the network society." While

this study is insightful because it draws focus to the potential of the internet to offer a new form of society, the depiction of power and counterpower in Castells study do not take into account the various ways in which the internet poses ontological security risks to states and venues of counterpower.

Countertechnologies, according to Steele (2010), "contain the ability to expose power to be, if not out of control, at least aesthetically frayed at the edges and indeed insecure, ambiguous, and indeterminate" (52). Technological counterpower, in the form of information flows and image dissemination has replaced material threats from counterpower as a primary vehicle for challenging the aesthetic integrity of centralized power (Steele 2010: 51). Steele (2010) notes that the internet "…is a much more unpredictable medium than television or radio forms of communication and thus naturally evokes counterpower possibilities and realities" (52). Instances of counterpower that center themselves, intentionally or unintentionally, around challenges to aesthetic power and the Self-identity of the state, have a much more lasting and potentially subversive possibility, because traditional state power cannot necessarily be tackled. Rather, information flows can constantly engage the state and force the state to legitimate its behavior and to deal with contradictions that arise between what state self-image and state physical security.

iv. Conclusion: Ontological Security and Aesthetic Power: Why Does This Matter?

Cyberspace is quickly becoming one of the most widely discussed issues facing nation-states. Popular accounts of cyber war and cyber security receive quite a bit of mainstream press.[15] James Clapper, the United States Director of National Security, argued in March of 2013 that cyber terrorism and cyber espionage have supplanted terrorism as the largest threat to

[15] Clarke (2010 and Singer (2014), for instance

U.S. national security.[16] Threats are portrayed as viruses, cyber attacks, espionage, and the like. Meanwhile, widespread data collection and surveillance by the National Security Administration portray a second face of cyber threat: attacks on personal liberty and privacy. While the threats that face states in the way of hacking, viruses, espionage, wide scale cyber attacks, etc. are certainly worth studying in their own right, little attention is paid to the various other ways cyberspace poses risks to states. The aim of this chapter is to lay a theoretical framework from which to examine cyberspace's challenge to states in terms of a state's ontological security. Part of the story being told here is that states engage in aesthetic practices of power which require constant upkeep. Why is ontological security important in understanding state behavior in cyberspace? How does cyberspace pose aesthetic challenges to state power? The significance of state ontological insecurity and aesthetics of power in cyberspace can be seen through the seemingly contradictory behavior of the United States in cyberspace.

What follows is an account of the ontological insecurity faced by the United States in cyberspace. Beyond the significant material threats posed by cyberspace, state justification for contradictory behaviors and practices sheds light on an alternative conception of state behavior in international relations: the pursuit of ontological security and an aesthetic of power. State projections of power in relation to cyberspace leave contradictions between liberty and security, and state identity and self-image that can be exploited through counterpower.

[16] See Reuters' description here: http://www.reuters.com/article/2013/03/12/us-usa-threats-idUSBRE92B0LS20130312 (Accessed 12 March 2014)

Chapter 3: Discourse Analysis in International Relations

This chapter examines official state discourse by the Obama Administration in an effort to examine how the state conceptualizes cyberspace and how contradictions between state self-identity and self-image are mediated through official discourse. A second focus of this chapter is a case-specific study of the U.S. official reaction to the disclosures made by former National Security Administration (NSA) contractor Edward Snowden. The focus on the NSA leaks by Snowden, and his appearance at the South by Southwest (SXSW) conference relate back to the complicated, and often contradictory, nature of the United States in relation to cyberspace. This chapter defines discourse, and the importance of discourse analysis in the study of international relations. Language, understood as an extension of state power, is open to challenges, just as state identity and self-image. To examine the ways the state, in this case the United States, is ontological insecure requires unpacking the discourse surrounding the United States in relation to cyberspace and the Snowden disclosures, because language and representations that state agents deploy regarding cyberspace is one of the few ways that the state can actively attempt to exert power with regards to its own ontological (in)security. Cyberspace, perhaps ironically, provides such a vehicle for state agents to go about securing the self identity and self-image of the state, through assertions of what cyberspace ought to be and narratives of legitimacy surrounding state action.

Discourse is important in the context of this study because discourse (defined shortly) illuminates not only what is thought and said, but the role that things which *are not* thought and said play in shaping cyberspace and securing state identity and self-image. Further, examining official state discourse, particularly how cyberspace is constructed and defined by the state, unearths underlying explanations for seemingly contradictory behavior in cyberspace. In other

words, in order to examine the relationship between state security and cyberspace, one must take into account not only the ways in which the state interacts with other states (in structural terms) regarding cyberspace, but also how the state comes to understand its own identity in the digital age.

i. Discourse and the Analysis of Discourse

What is discourse? Adam Hodges (2011: 6) defines discourse as "language use." Hodges goes further, citing Hall (1997: 44), and adding a Foucauldian dimension to discourse: "[a] way of representing the knowledge about […] a particular topic at a particular historical moment." Hodges (2011: 6) adds: "…a discourse regulates the way a topic can be talked about meaningfully in a particular culture at a particular point in history." Jim George (1994) describes the power of discourse analysis to "…illustrate how […] textual and social processes are intrinsically connected and to describe, in specific contexts, the implications of this connection for the way we think and act in the contemporary world."[17] Here, it is important to note the different conceptions of discourse analysis, helpfully organized by Gee (2005) between 'little d' and 'big D' discourse: linguistic versus cultural domains of language (Foucaldian), respectively (Hodges 2011: 7).[18] 'Little d' and 'big D' discourses, according to Hodges (2011:7), are linked through a critical discourse analysis (CDA) approach, first posited by Fairclough (1992). Here, micro-level elements of discourse (linguistic), the situated use of language, are related to larger macro-level discourses (Hodges 2011: 7).

[17] Cited in Milliken (1999)

[18] This is not to suggest that either 'little d' or 'big D' discourses are mutually exclusive, or the only understandings of discourse. For instance, discourse, according to Kathy E. Ferguson (1987: 209), is "…the characteristic ways of thinking and speaking that both constitute and reflect our experiences by illuminating certain roles, rules, and events while leaving others unnamed."

ii. Discourse Analysis in International Relations

Jennifer Milliken (1999: 226) notes that scholars who use discourse analysis in international relations have tended to avoid methodological questions attached to discourse analysis. This, Milliken argues, stems from the neopositivist and rationalist scientific theories of mainstream international relations, and the perceived preoccupation with methodology by mainstream IR scholars (1999: 226). However, this "scant attention" to methodological questions surrounding discourse analysis, Milliken suggests, places the approach at a disadvantage (1999: 226).

There are three bundles of theoretically distinct commitments that Milliken (1999) uses to discuss and organize the study of discourse in international relations: discourses as systems of signification, discourse productivity, and the play of practice (229-230). In the first "bundle," discourses construct social realities through, for instance, relationships or binary oppositions (229).[19] Here, (material) things do not convey the meaning of the social world. Rather, the social world is constructed by people, through language, images, etc. Of particular interest is the second "bundle"—a theoretical commitment to discourse that understands discourse's productive capacity to make meanings about the world through operationalization and authorization (229). Milliken (1999: 2009) notes: "…of significance for the legitimacy of international practices is that discourses produce as subjects *publics* (*audiences*) *for authorized actors*, and their *common sense* of the existence and qualities of different phenomena and of how public officials should act for them and in their name (e.g. to secure the state, to aid others)."

Discourses can restrict and exclude, or define and enable (Milliken 1999: 229). The third "bundle" of theoretical commitments in the study of discourse in international relations is the

[19] Milliken references Saussure and Derrida, respectively here

commitment to understanding all discourse, even hegemonic discourse, as unstable and thus in constant need for discourse to rearticulate knowledge and identity (230). This constant need to articulate and rearticulate can be paralleled to the notion that states must maintain/reproduce their self-image in order to have some sort of ontological security.

Articulation demonstrates agency and, as Hodges (2011: 6) notes, discourse "regulates the way a topic can be talked about meaningfully…" Cracks in discourse emerge from articulation and rearticulation. Similarly, the need to maintain a self-image and an aesthetic of power ultimately leads, as Steele (2010: 6) notes, to more insecurity. However, the cracks in discourse, the contradictions of self-image, and the challenges to power are only the beginning of the story. What is at stake in this analysis are the meanings produced to "cover up" the "cracks" in discourse, the ontological insecurity of the state in the face of contradictions to self-image, and the weaknesses that projections of strength ultimately draw attention to. This, in part, explains state justification for surveillance, violence, and exploitation in the name of stability and an idealized self-image. Roxanne Doty (1993: 298) argues that foreign policy analysis must go beyond explaining *why* decisions are made, and instead focus on *how-possible* questions. Doty (1993: 298-299) argues:

> In posing such a question, I examine how meanings are produced and attached to various social subjects/objects, thus constituting particular interpretive dispositions which create certain possibilities and preclude others. […] How questions, so posed, go to an important aspect of *power* that why questions too often neglect. They go to the way in which power works to constitute particular modes of subjectivity and interpretive dispositions.

States narrate about themselves through the discourse of state agents. State actions must be justified, even if they go against the grain of international norms or expectations (Steele 2008: 10). According to Lang (2002), "only in the telling of the event does it acquire meaning, the

meaning that makes such events politically relevant."[20] According to Steele, the biographical narrative of a state is constituted by a connection, through the telling of an event, between a policy and a description or understanding of the state's self (2008: 10). State narrative is thus crucial, according to Steele: "Narrative is the locus from which we as scholars can begin to grasp how self-identity constrains and enables states to pursue certain actions over others" (10). Importantly, narrative brings to light a parallel between the *meanings* of state action and state identity (11). In other words, no matter how incongruent, puzzling, or seemingly nonsensical state behavior may be, an analysis of the meanings actors create in the way of justification should line up with the self-identity of the state.

Discourse analysis provides three ways to connect state behavior to the self-identity of states (Steele 2008: 12). First, using discourse analysis can uncover state justifications by looking from the perspective of the policy/behavior back to self-identity (ibid.: 12). Second, looking from the perspective of the self-identity of the state, discourse analysis can illuminate when self-identity leads to policy decisions (ibid.: 12). Finally, discourse analysis "…uncovers how the actors create meanings not only of their vision of state self-identity but also of identity threats (what "causes" them, why those threats must be dealt with, which policy can best confront these threats, etc.)" (Steele 2008: 12). With respect to this study of cyberspace and the ontological insecurity of the state in confronting cyberspace, discourse analysis can illuminate how the United States creates a particular set of meanings vis-à-vis cyberspace that could show how not only how the United States views itself, as a state, in relation to cyberspace, but also what sort of threats cyberspace poses in the way of self-identity. Hansen (2006: 21) notes the use

[20] Cited in Steele (2008: 10)

of language in constructing policy, which lends itself well to Steele's (2008) three objectives of discourse analysis:

> The conceptualization of foreign policy as a discursive practice implies that policy and identity are seen as ontologically interlinked: it is only through the discursive enactment of foreign policy, or in Judith Butler's terms 'performances,' that identity comes into being, but this identity is at the same time constructed as the legitimization for the policy proposed.

David Campbell (2003: 57) notes: "If we assume that the state has no ontological status apart from the many and varied practices that bring it into being, then the state is an artifact of a continual process of reproduction that performatively constitutes its identity. The inscription of boundaries, the articulation of coherence, and the identification of threats to its sense of self can be located in and driven by the official discourses of government." Thus, ontological insecurity in terms of cyberspace can be located within the discourse surrounding cyberspace. This 'performance' by states, in this case the United States, reveals the constitutive makeup of state identity, and its power, understood as its ability to recreate or operate upon its self-image.

iii. Case Selection

This thesis examines key documents prepared by the Obama Administration involving cyberspace, Cyberspace Policy Review (2009) and International Strategy for Cyberspace (2011), along with a series of speeches made by President Obama and Vice President Joe Biden that inspired these white papers, or that respond to cyberspace and national security. Cyberspace Policy Review (2009) and International Strategy for Cyberspace (2011) both represent key policy documents that have emerged fairly recently from the White House, and represent two competing messages regarding the United States and cyberspace. Thus, the documents provide a useful comparison that demonstrates the navigation between state physical security and state self-image. The speeches from President Obama and Vice President Joe Biden form part of a

larger official state discourse on cyberspace, and demonstrate contradictions in message and rhetoric. These speeches are framed on either side of a moment, what will later be described as an 'aesthetic irruption:' Edward Snowden's leaks regarding the mass surveillance by the NSA. This event also offers before and after comparisons for purposes of demonstrating how ontological insecurity can be viewed in the discourse of state agents. Finally, chapter three ends with an analysis of Edward Snowden's appearance at the South by Southwest (SXSW) conference, visually examines his appearance at the conference, and examines how the state deals with this 'aesthetic irruption.' The inevitable question, 'why the United States' is also addressed in the following chapter. In short, the United States, as a state, offers a quite unique set of characteristics that make it especially prone to ontological insecurity: militarily dominant, yet by way of history and foundational elements, easily contradicted.

Chapter 4: The NSA Leaks, Ontological Insecurity, and the Self-Image of the United States

i. Introduction

Aesthetic power is the ability to maintain or reconfigure self-image. Ontological insecurity hides itself in state discourse about cyberspace, in contrast to physical insecurity, which states can leverage to provide justification for intrusion into cyberspace that can seemingly run counter to the self-image the state wishes to maintain in world politics. What the United States envisions cyberspace ought to be, and how the United States comes to understand its own identity and self-image in relation to cyberspace form the bulk of the analysis in this chapter. The ways in which cyberspace becomes defined in key documents and official state discourse of the United States demonstrate how U.S. identity and self-image are understood in relation to cyberspace. Further, this chapter examines how the state attempts to deal with the tension between liberty and security in cyberspace through claims of American exceptionalism, conceptions of shared American values, ahistorical references to the past, and deflections of responsibility for state actions. These attempts, I demonstrate, bring about contradictions in the official state discourse surrounding the United States and its relationship to cyberspace, because mediating the liberty/security dilemma is seemingly unreachable for the state. State agents, through language, as an extension of state power, attempt to work through these dynamics. These attempts, and the contradictions that arise, ultimately leave the state vulnerable to challenges to its self-image and identity in relation to cyberspace, and demonstrate weaknesses in policy, security, and, in the end, the ability of the state to live up to its own purported identity and self-image.

This chapter examines key documents prepared by the Obama Administration involving cyberspace, Cyberspace Policy Review (2009) and International Strategy for Cyberspace (2011),

along with a series of speeches made by President Obama that inspired these white papers, or that respond to cyberspace and national security. There are many tensions and contradictions that arise throughout these documents and speeches; Cyberspace Policy Review, written under the auspices of the protection of domestic infrastructure, contrasts well with the International Strategy for Cyberspace, which takes on a more conciliatory tone towards the benefits of cyberspace, but still attempts to qualify and mollify contradictions related to self-image and an aesthetic of power. The speeches made by President Obama regarding cyberspace highlight further this critical need for states to maintain a self-image in light of what Steele (2010: 51) calls "aesthetic irruptions." To this end, the chapter finishes with an examination of statements made after the NSA disclosures by Edward Snowden in 2013, with further analysis of Edward Snowden's appearance at the South by Southwest (SXSW) conference. The aim of this chapter is to show how ontological insecurity, through official state discourse that is riddled with contradictions, and that maintains or reconfigures state self-image in light of aesthetic irruptions, creates conditions which can be used by states as justification for intrusion into cyberspace and that frame cyberspace in the language of security and militarization.

ii. Defining the Self-Identity and Self-Image of the United States

When examining speeches made by U.S. state agents, publications regarding U.S. citizenship, and the ways the United States is presented in popular culture, common trends emerge; the United States is presented as exceptional, as a *land* of shared values, including liberty, freedom, and prosperity, and as a country based upon foundational elements created by the nation's founding fathers. David Campbell (1998: 131) suggests that the United States is an imagined community "par excellence." The United States, like all other states, is dependent upon practices that make up its ontological being. However, Campbell (1998: 91) argues:

"Defined, therefore, more by absence than presence, America is peculiarly dependent on representational practices for its being. Arguably more than any other state, the imprecise process of imagination is what constitutes American identity." Space and time in reference to U.S. identity is crucial to this analysis, because a fulfillment of ontological security for a state is predicated upon its ability to maintain a consistent self-identity and self-image. Void of a people as a foundational element, the United States' self-identity is quite fleeting, and, thus, hinges on representational, symbolic, and iconic imagery in order to ascribe to itself some form of identity (Campbell 1998: 132). Former President George W. Bush (2001), in a similar vein, remarked during his inaugural address that:

> America has never been united by blood or birth or soil. We are bound by ideals that move us beyond our backgrounds, lift us above our interests and teach us what it means to be citizens. Every child must be taught these principles. Every citizen must uphold them. And every immigrant, by embracing these ideals, makes our country more, not less, American.[21]

The contradictions that arise in narratives surrounding cyberspace, in which state agents seek to stay true to universal values in the face of very particular and real foreign policy and security practices, create contradictions that need to be remedied (Campbell 1998: 131). This arises in the forthcoming analysis through narratives of American exceptionalism, the preservation of values such as individual liberty and personal privacy, and in ahistorical or anachronistic references to the past in order to justify present circumstances. These narratives can help explain not only responses to quite obvious contradictions and aesthetic irruptions, but also show how ontological (in)security creates conditions and justifications under which

[21] Transcript of President Bush's address can be found here: http://www.presidency.ucsb.edu/ws/?pid=25853 (Accessed 7 May 2014).

particular state actions in cyberspace run counter to what America *should* be doing with respect to its own self-identity.

iii. Defining Cyberspace

In order to discuss cyberspace in terms of national defense strategy, economic initiative, technological innovation, etc., the White House defines what it believes cyberspace *is*, or what it *ought to be.* In this study, it is not necessarily important to create or justify a particular definition of cyberspace, because cyberspace, with respect to state (in)security, is what states make of it. These attempts in the Cyberspace Policy Review and the International Strategy for Cyberspace to lay out how the United States comes to understand cyberspace is an extension of state power in two ways. First, in arguing for a particular manifestation of cyberspace, the United States, as a global leader, attempts to create a universal 'nature' of cyberspace. Second, and for this study more importantly, inherent in the definitions of cyberspace proposed by the White House are contradictions in what cyberspace is and ought to be, which highlights the tension between state identity and self-image, on the one hand, and the tension between liberty and security, on the other. In terms of a comparison between two White House documents related to cyberspace, the Cyberspace Policy Review and the International Strategy for Cyberspace, there are some distinct differences in the representation of what cyberspace is to the state. The Cyberspace Policy Review defines cyberspace as:

> …the interdependent of network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. (1)

In contrast, the International Strategy for Cyberspace does not posit an explicit definition of cyberspace. Rather, a vision of cyberspace emerges from the document:

> The United States will work internationally to promote an **open, interoperable, secure, and reliable** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, we will build and sustain an environment in which **norms of responsible behavior** guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[22] (8)

There is a stark difference in the tone set by each document, particularly when it comes to what cyberspace is and what cyberspace should be about. On the one hand, Cyberspace Policy Review represents a routinized response to a new threat. Granted, the document does contain calls to change the status quo, but these calls are still directed towards the same "football play manual" that states use to address issues of security.[23] On the other hand, the International Strategy for Cyberspace attempts to fit cyberspace within broader goals that are grounded in self-image, or what the document calls "grounded in principle." The manner in which each document posits a definition of cyberspace is important; viewing cyberspace as a network of infrastructure that needs protecting carries with it a justification for the securitization of cyberspace, while cyberspace as a platform for innovation implies that cyberspace is compatible with the self-image of the United States as free and open. Daniel R. McCarthy (2011: 105) argues that the way the Internet is characterized by the United States is ultimately an attempt to define, in line with U.S. interest—but posited as an international norm—what the Internet *should be*:

> The argument of US foreign policy officials, that an Internet characterized by the free flow of information meets international norms of human rights and democracy, is an attempt to steer the development of the technology in a direction that meets its specific vision of how international society should function. By defining the technology as meeting those aims only if designed and used in line with US foreign policy aims, American officials are enacting a form of technological closure, drawing creatively upon the symbolic resources of international society in the process.

[22] Emphasis in original
[23] Routine will be addressed shortly in this chapter

This finding fits well with the International Strategy for Cyberspace's definition of cyberspace, and with the United States' understanding of its desired self-image: open and free. Further, it also fits the strategic goals of the United States regarding cyberspace. The 'symbolic' resources of international society that the United States draws upon are justified in what is ultimately an expression of U.S. material power: "As a form of power, this ability to shape the design of technology possesses an almost unprecedented geographic reach and historical scope" (McCarthy (2011: 105). Furthermore, the expression of what the Internet ought to be, harkening back to what the United States ultimately believes its role is internationally, is an attempt to secure the self-identity and self-image of the state. In other words, as Mitzen (2006: 354) explains, ontological security places some explanation between states, in inter-state routines. Cyberspace is not an 'American' thing, but the United States seeks to exert some control over what cyberspace is and ought to be, and in doing so, attempts to reinforce ontological security under the guise of international cooperation and society.

iv. Contradictions

President Barack Obama's remarks on cyberspace on May 29, 2009 illustrate some of the problems of transference when states try to replicate or maintain their aesthetic image and power in cyberspace. One of the opening statements in Mr. Obama's speech makes it very clear that he believes that a virtual world exists, and that it is fundamental to the country's functioning daily life:

> It's long been said that the revolutions in communications and information technology have given birth to a virtual world. But make no mistake: This world -- cyberspace -- is a world that we depend on every single day. […] So cyberspace is real. And so are the risks that come with it.

State mediation of the uncertainty and threat generated by cyberspace can be understood in terms of the complicated nature of cyberspace as a deterritorialized 'space.' Cyberspace presents a new kind of domain of interaction for states, a domain that perpetuates physical insecurity (in the way very real and uncharted threats) and ontological insecurity (in the way of an uncertain and constantly shifting self-image). U.S. domination of sea, air, land, and space hinges on a conception of power and security that is material strength and physical dominance. Kuehl (2009: 29) argues that cyberspace is often described as a new operational space. Similar to the other operational domains of land, sea, air, and space, cyberspace is thus painted as a bounded space in which national security actors, as well as other state and non-state actors, can operate. The inclusion of cyberspace into the mode of thinking that demarcates operational arenas for domination shows itself in the ways in which states talk about cyberspace; seemingly absent of self-reflexivity, states have routinized responses to cyberspace that miss, or try to navigate, the ontological insecurity that cyberspace breeds. This routinization "imposes cognitive order on the environment" in order to shield the state from uncertainty (Mitzen (2006: 346). Uncertainty, and its relationship to routine, appear in Vice President Biden's remarks at the London Cyberspace Conference in 2011:

> Of course, cyberspace presents challenges that are different from any we've faced before, and it raises new questions. It forces us to come up with new approaches where old ones no longer suffice. Consider confidence-building measures. It's a great deal harder to assess another nation's cyber-capabilities than to count their tanks, for example. Governments don't have a monopoly on it, and we can't -- you can't judge the intentions of another country by looking at its force -- like by looking at its force posture. So it's a challenge to identify effective, confidence-building measures in cyberspace. We've got to find a way.

Under the auspices of a UK cyberspace conference, the Vice President acknowledges frustration due to a lack of concrete confidence-building measures in cyberspace. Confidence-

building measures are grounded in routine. In addition, the Vice President signals that capability in cyberspace is unknown (and will probably remain unknown). This notion that cyberspace lacks effective ways to identify threat and capability in cyberspace from Biden can be contrasted against an earlier speech made by President Obama in 2009, where routine, coupled with rhetoric of control is voiced by the President:

> From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

In "traditional" conflict, state actions may seem contradictory from a strategic standpoint, but through an understanding of ontological security, strange actions by the state can be understood as an attempt to preserve a particular self-image. Further, the aesthetic of it all, what states "look like," by way of their own self-image, can explain what operational analyses cannot (Gould and Steele 2014). The mediation of contradiction, liberty for all but death to some, arises not in the justification for strategy, but in reference to a greater good (a reflection of self-image). The problem of mediation is amplified in cyberspace because state self-image is constantly shifting in what President Obama notes is an information age in its infancy:

> But we need to remember: We're only at the beginning. The epochs of history are long -- the Agricultural Revolution; the Industrial Revolution. By comparison, our Information Age is still in its infancy. We're only at Web 2.0. Now our virtual world is going viral. And we've only just begun to explore the next generation of technologies that will transform our lives in ways we can't even begin to imagine.

The rhetorical deployment of ownership and control over cyberspace represents an intentional posturing aimed at cyberspace's many constituents: other states, non-state actors, firms, etc. Terms of control, security, trust, and resilience are believable in traditional classical-

realist accounts of international politics, where the United States has been an economic hegemon and military giant. However, the rather sudden emphasis on cyberspace as an issue of "high politics"[24] and the growing rhetoric attached to threats coming *from* cyberspace (cyber war, cyber terrorism, cyber currencies, etc.)[25] very quickly dissolve the façade surrounding U.S. power to actually secure itself against the threats coming from cyberspace. The doubt surrounding the United States' ability to control its interests adequately in cyberspace do not arise simply from its own rhetoric, but rather, clear instances of vulnerability in the form of *real* attacks from diverse arenas such as other states, local governments, private companies, and individuals. It is worth noting that governments are quick to demonstrate the dangers of threats coming from cyberspace, and also posit cyberspace as a causal factor in "real" world crime.

Crucially, the security of the United States in the 21st Century hinges upon its own self-image. While the ability of the United States to carry out attacks in traditional domains of operation: sea, air, land, and space is virtually unquestionable, cyberspace poses a new kind of threat to a new kind of vulnerability in global politics. Steele (2014) notes: "It is easy to tweak someone that has this idealized understanding of who or what they are. It is harder to tweak someone at an individual level who doesn't really give a damn about what he looks like. But you can inherently and quickly, momentarily at least, tweak or cajole or insecuritize an actor that focuses on crafting an aesthetic self." The defense, preemptive or reactionary, of particular behaviors in cyberspace that seem contradictory to an idealized self-image are found throughout official discourse on cyberspace. This defense is also an attempt to balance the quite obvious contradictions between security and liberty, control and open access. President Obama argues:

[24] See Choucri (2012)
[25] See Clarke (2010), Singer (2014)

> Let me also be clear about what we will not do. Our pursuit of cybersecurity will not -- I repeat, will not include -- monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties that we cherish *as Americans*. Indeed, I remain firmly committed to net neutrality so we can keep the Internet as it should be -- open and free.[26]

President Obama's remarks make it apparent that the United States must balance national security and liberty in cyberspace, a common tension that states face in other aspects of governance. However, there is a difference when states attempt to mediate national security concerns and personal liberty in cyberspace. President Obama sends two distinct and seemingly irreconcilable messages regarding cyberspace: first, the United States, as a centralized power, recognizes the tensions that it must mediate between security and liberty, and, second, that the United States has a vision for cyberspace, one focused on being "open and free." But free for whom? Steele (2008: 1-2) notes the binary of "self" vs. "collective" interest in security, and argues that Americans are generally left to choose between policies that are markedly selfish (in terms of international best-interest) yet reinforce American security, or policies that are popular internationally, yet leave something to be desired in terms of America's conception of its own physical security. Perhaps Obama's remarks indicate a recognition of material self-interest and existence as well as a social need, but what happens when, in an area such as cyberspace, securing a self-identity through time is seemingly impossible? What happens when the aesthetic self comes under serious scrutiny, in the form of global pressure to end massive surveillance regimes in cyberspace?

These remarks by President Obama also indicate a tension between the self-image of the United States as a sovereign nation-state, whose primary responsibility is that of guaranteeing liberty and security to its people, and a self-image that attempts to mediate an altruistic take on

[26] Emphasis added

its role in the world with a strategic one. American security policy is decentralized, insofar as it attempts to do too much while still trying to keep a constant self-image.[27] Cyberspace is not an "American thing," but from cyberspace comes a multitude of images that only exacerbate the imagined nature of American identity. Thus, what cyberspace *is* and what cyberspace *means*, from an American perspective, is inherently *American*.

v. Aesthetic Irruptions and Countertechnologies: State Response to Edward Snowden and the NSA Leaks

In June 2013, *The Guardian* newspaper printed a story that captivated and troubled many: the United States collects phone data from millions of its own citizens. The whisteblower, or traitor according to many, was Edward Snowden, a former National Security Administration contractor (BBC 2013). Quickly, the scope and scale of the data collection practices of the NSA came under scrutiny; Snowden released information to *The Guardian* that indicated that the NSA hacks Chinese networks, bugs offices of the European Union, screens calls from German Chancellor Angela Merkel, and collects more than 200 million text messages a day (BBC 2014). These leaks represent a micropressure, exacerbated by countertechnology, that de-aestheticizes the self-image of the United States.

What happens when the aesthetic construction of centralized power is de-aestheticized, such as in this case of massive data collection? Counterpower is a micropressure (Steele 2010: 2). Such micropressures require a response, and in this case, the response is twofold. First, Edward Snowden, the figure of the micropressure, must be addressed in a particular way.[28] Second, the narrative that arises from the state must seek to legitimate behavior that either runs counter to self-image, or counter to a reasonable strategy of security. In this case, the narrative

[27] See Campbell (1998) ; Gould and Steele (2014)
[28] The merits, or lack thereof, of Snowden's actions are beyond the scope of this paper.

justifies behavior that is strategic, but that runs counter to self-image.[29] Countertechnologies, according to Steele (2010:52), "contain the ability to expose power to be, if not out of control, at least aesthetically frayed at the edges and indeed insecure, ambiguous, and indeterminate." Technological counterpower has replaced material threats from counterpower as a primary vehicle for challenging the aesthetic integrity of centralized power (Steele 2010: 51). Instances of counterpower that center themselves, intentionally or unintentionally, around challenges to aesthetic power and the Self-identity of the state have a much more lasting and potentially subversive possibility, as seen in the reaction to Snowden's release of classified information from the likes of German Chancellor Angela Merkel.

Addressing the "noise" surrounding the practices of the National Security Administration, President Obama first noted the history of intelligence gathering by the United States:

> At the dawn of our Republic, a small, secret surveillance committee, born out of the Sons of Liberty, was established in Boston. And the group's members included Paul Revere. At night, they would patrol the streets, reporting back any signs that the British were preparing raids against America's early patriots.

In order to find footing and precedent in the face of the aesthetic irruption and ontological insecurity, two rhetorical moves are deployed. First, history is resurfaced and reworked to create a seemingly appropriate metaphor for the present. This history is doused in a patriotic whitewash, whereby particular events are chosen but not others that are perhaps more indicative and relevant to the current situation. Further, the parallels that are put forward for consumption are not parallels at all; the nature of surveillance, global politics, globalization, and technology are not the same as they were 200 or so years ago. This history serves to maintain self-image

[29] This is different than, say, the Falklands War, where Britain had to justify the death of British men and women in the name of country (and ultimately, of Empire)

over time. Campbell (1998: 130) notes that the American quasi-war with France "demonstrated how previously established discursive strategies of otherness could be invoked in novel circumstances to provide powerful modes of understanding." Much in the same way, this return to history by President Obama serves not only to ground justification in seemingly consistent practices of state surveillance, but also to an "other," in this case, the British during the Revolutionary War. Threat from cyberspace comes from a plethora of different sources, including other states, non-state actors, rogue Americans, or even cyberspace itself. The second rhetorical move is to argue for American exceptionalism:

> But America's capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do. That places a special obligation on us to ask tough questions about what we should do.

The justification for (at least toned down) policies of surveillance by the NSA is centered on the notion that "someone has to do it," and "we can do it better than anyone else." American identity, as "the world's only superpower," as President Obama declares, opens itself up for interrogation. As Steele (Gould and Steele 2014) notes: "If you think about the cosmetic angle to it, it is making you look like something else than you think you are. You have an idealized representation of what you should look like and you're constantly trying to strive for that. But just like supermodels and airbrushing or whatever else, there is no way you can strive for that all the time. So you are inherently set up to be insecure, and that's the meaning of insecurity."[30] American exceptionalism certainly did not begin with the digital age; Daniel Bell (1975: 195) argues that American exceptionalism goes as far back as the initial exploration of the Americas: "But there was also the thought that America was not just one more empire in the long chain of men's pursuit of domination, but a transforming presence whose emergence at the center of

[30] Steele goes on to qualify the meaning of insecurity he mentions as simply one take on insecurity

history had been made possible not only by the providential wealth of a virgin continent but by the first successful application of a new principle in human affairs." Bell (1975: 211) goes on to suggest that the United States has largely escaped a problem of security that many others have faced: foreign invasion/war on their own soil. This, written in 1975, is perhaps less true given the changing nature of a globalized world, particularly post-9/11. However, pushing Bell's original claim further, American exceptionalism, with regards to a detteritorialized space in cyberspace, is threatened by the very nature of cyberspace: cyberspace is ubiquitous. Thus, American capability must be more ready to address the (physical) threats of cyberspace, while living up to its self-identity and self-image. Does the "world's only superpower," as President Obama refers to the United States, have the cyber capability to adequately live up to a label that, up until now, rings true?

> We cannot prevent terrorist attacks or cyberthreats without some capability to penetrate digital communications, whether it's to unravel a terrorist plot, to intercept malware that targets a stock exchange, to make sure air traffic control systems are not compromised or to ensure that hackers do not empty your bank accounts. **We are expected to protect the American people; that requires us to have capabilities in this field**.

Thus, President Obama essentially securitizes the American people as justification for state action in cyberspace. The rhetoric changes; cyberspace, according to President Obama in 2009, should be "kept" open and free, but the limitless, mysterious, enemies that come from cyberspace require the United States to, in the name of the American people, to exert vague capability (capability that Vice President Joe Biden describes as limitless and difficult to measure). President Obama goes on to argue:

> No one expects China to have an open debate about their surveillance programs or Russia to take privacy concerns of citizens in other places into account.

President Obama's comments on Chinese and Russian state surveillance practices can be understood in terms of the self-image of the United States as well. Self-image is, in part, based around the idea of what the self *is not*. The sentiment, that the United States' behavior is in direct opposition to that of China and Russia, is perplexing; until the Snowden leaks, there was no debate about NSA surveillance of citizens. The gesture towards states who are seemingly opposite by way of self-image is an instinctive reaction to aesthetic irruptions and of ontological insecurity. It is a deflection of not only responsibility, but of an alternative depiction of the self. Steele (2010: 31) argues that in search of self-image, states narcissistically seek reflections of themselves in the behavior of others, such that "each action that occurs "out there" *must* say something about the Self."[31] However, there is a danger in seeking out reflections of the self in others. This speech by President Obama was criticized, and in some cases mocked, by commentators such as John Stewart on *The Daily Show* for the inherent hypocrisy throughout the speech with headlines like "Privacy Important Until We Decide It Isn't."[32] Hence, there is a vulnerability in searching out the self in others: which version of the self will emerge?[33] This harkens back to the central claim of this thesis: the state is ontologically insecure in relation to cyberspace, and attempts to mediate the contradictions between self identity and self-image, on the one hand, and state practices, on the other, only exacerbate ontological insecurity through portrayals of such contradictions in official state discourse and practice.

[31] Emphasis in original
[32] See video of the segment at http://www.realclearpolitics.com/video/2014/01/21/jon_stewart_mocks_obamas_nsa_speech_privacy_important_until_we_decide_it_isnt.html (Accessed 12 March 2010)
[33] See Steele (2010: 31)

vi. Speed and Ontological Insecurity in Cyberspace

At the end of his speech on NSA reforms, Barack Obama demonstrates, perhaps unintentionally, that ontological insecurity is a powerful motivator for the United States in cyberspace:

> **When you cut through the noise, what's really at stake is how we remain true to who we are in a world that is remaking itself at dizzying speed.** Whether it's the ability of individuals to communicate ideas, to access information that would have once filled every great library in every country in the world, or to forge bonds with people on the other side of the globe, technology is remaking what is possible for individuals and for institutions and for the international order. So while the reforms that I've announced will point us in a new direction, I am mindful that more work will be needed in the future. One thing I'm certain of, this debate will make us stronger. And I also know that in this time of change, the United States of America will have to lead.[34]

This is not to say that the United States consciously and reflexively recognizes its ontological insecurity in its relationship to cyberspace, but that the examples that are posited concerning the dangers of cyberspace, from cyberspace as a mechanism for terrorist mobilization to cyber wars of the future, do not paint an entirely clear picture of what makes cyberspace something truly different in global politics. This shift is not universal, or at least to the same degree, for every state; cyberspace may provide a vehicle for dissent, organization, etc. for every state, but it burdens states who are fixed in terms of physical security and depend on an idealized image of who they are, such as the United States.

Speed, by way of globalization, is not a new phenomenon. However, the degree to which interaction occurs at a blistering pace in cyberspace is. Kinnvall (2004: 742) notes this effect of globalization to compress time and space. Kinnvall (2004: 742) argues: "…in terms of cognition, there is an increased perception of the globe as a smaller place—that events elsewhere have consequences for our everyday political, social, and economic lives, affecting individuals'

[34] Emphasis added

sense of being." While Kinnvall focuses on the ontological security of the individual in a globalized world, the same can be said of the state in relation to cyberspace; cyberspace's ubiquitous nature, coupled with its permeable, temporal, (a)physical, and fluid attributes creates a condition under which states, as President Obama notes, are adapting to a world that is "remaking" itself at a dizzying pace.[35] This near instantaneity of life, for those who are "plugged in" to digital life, or who are tangentially impacted by cyberspace, creates a need to search for, or cling to, space and time-bound identities.[36] Globalization is thus connected to security, or insecurity, through globalization's dislocating nature (Kinnvall 2004: 744). Cyberspace's ever-present nature draws the state into different area of interaction, through which identity cannot be grounded in space or time-bound identities.

President Obama rightly indicates the important nature of speed with respect to a world that is becoming increasingly interconnected. Speed plays another important role to state insecurity in cyberspace; void of a centered self-image to begin with, and an aesthetic self that is contingent upon a stable self-image, speed intensifies ontological insecurity. Thus, the President of the United States is called upon to make note of speed and the difficulty in remaining "true to who we are." This extends beyond a shifting or decentralizing identity and into the inherent powerlessness in it all; the United States is powerful, by way of traditional conceptions of power, but is beholden to its self-image and self-identity that is easily manipulated. The "superpower" of good suddenly is cast as "Orwellian" by virtue of its large data-gathering program. The President must hold in one hand the ideals of democracy and liberty that make American identity and the security and dominance that "makes America strong" in the other hand. Beholden to

[35] See Choucri (2012: 4) for an analysis of the characteristics of cyberspace
[36] Kinnvall (2004) cites Harvey (1989: 4) in reference to the search for ways to cope with these effects on modern life.

these contradictions, the dissemination of information and of counter self-images projected back upon the state is done at great speed. The gaze of the world requires the maintenance or rearticulation of self-image out in the open. The process is messy; projections of strength (in relation to cyber capability) focus attention on perceived weakness, and also contradict the ideal self-image.

vii. Snowden on Screen at SXSW: Visual Irruptions of State Self-Image

On Monday, 10 March 2014, Edward Snowden appeared on a large video monitor to reach out to attendees of the South by Southwest (SXSW) festival in Austin, Texas. Rerouted through dozens of proxy servers, Snowden discussed how the NSA uses its surveillance capability to reportedly spy on its own citizens and those abroad.[37] In what is perhaps more interesting than Snowden's remarks at SXSW, Snowden appeared on webcam with a full screen mockup of the U.S. Constitution behind him. This visually striking image, of a man labeled a traitor by some and whistleblower or even a hero by others, carries with it a series of meanings that warrant further investigation with respect to how aesthetic irruptions destabilize the self-image and ultimately the ontological security of the state.

Visual analysis in international relations and security studies can lend itself well to a broader analysis of discourse and meanings that occur by way of cyber discourse. What is important regarding the image of Edward Snowden with the Constitution of the United States in the background is not the meanings that the image generates on its own, but rather, the intertextual context of the image as an intentional gesture by Snowden to send a particular message to a global audience. Counterpower, in this regard, meets the state on its own self-

[37] Find a description of the conference by *The Guardian here:* http://www.theguardian.com/world/video/2014/mar/10/edward-snowden-talks-nsa-internet-surveillance-sxsw-video (Accessed 11 March 2014)

constructed terms (Steele 2010: 47). The message, through the medium under which the state is ontologically insecure, cyberspace, goes beyond what Snowden says and shines light on the aesthetic irruption, placing the Self of the United States under a (micro) pressure. Hansen (2011: 53) notes four components to inter-visual/intertextual analysis: "the image itself, its immediate intertext, the wider policy discourse, and the texts ascribing meaning to the image." However, insofar as Hansen (2011: 52) is concerned with how images 'speak security,' this examination harkens back to ontological insecurity as states confront challenges to self-image. As such, this analysis theorizes how this particular image of Edward Snowden comes to 'speak counterpower.' This example speaks not only to a particular aesthetic irruption of state self-image and identity in cyberspace, but to the possibilities that cyberspace allows for forms of resistance to the state that meet the state on its own narrative terms in relation to state identity and self-image.

Situated within the wider discourse, Snowden's choice of backdrop can be understood in two ways. First, whether intentional or not, the image can be understood as a challenge to the United States' self-image; Snowden is perhaps trying to represent himself as the contradiction to what the United States holds to be an idealized self-identity and self-image. In other words, the background represents the idealized self-image of the United States, harkening back to Campbell's (1992: 132) notion of the United States' self-identity as fleeting and hinging on symbolic or iconic imagery. In the foreground, Snowden represents counterpower by way of countertechnology. The second interpretation of Snowden's choice of backdrop begs the question: does Snowden subscribe to an idealized self-identity as a citizen of the United States, and view himself as a defender of said self-identity in the face of what he understands as an irreconcilable contradiction to that self-identity by the NSA? Does the intention of Snowden

matter, or does meaning become ascribed to the image by the discourse surrounding Snowden, the NSA, and cyberspace?

Circulability is an important aspect to consider when examining visuals (Hansen 2011: 57). Here, circulability means more than passing from person to person, place to place; circulability involves the way an image is able to reach a broad audience in terms of meaning, speed in relation to circulabilty, and transgress language boundaries (Hansen 2011: 57). The Snowden image targets a particular audience: the American people. The image does very little by way of meaning transference to those who do not speak English and are unfamiliar with the U.S. Constitution as an image. However, the image, with respect to the constitutive members of the United States, sends a rather clear message, one that evades, to a certain extent, what David Campbell (2003: 59) refers to as "cultural governance;" the image circulated widely and quickly without a timely official response to Snowden's remarks. While cable news networks, the print media, etc. are more easily co-opted by the government to advance policy agendas, the internet holds no such promise by way of cultural governance. In a sense, what Snowden presents here is a counter-image that in some ways mocks the traditional image of centralized power, where agents of the state stand in front of iconic symbols such as flags, or in traditional, historic, rooms.

Snowden's strategy, more generally, and his choice of backdrop, more specifically, can be understood as rhetorical coercion (Krebs and Jackson 2007). Krebs and Jackson (2007: 36) propose a model of 'rhetorical coercion' in order to understand the role of rhetoric in politics. The authors argue: "While claimants may deploy arguments in the hope that they will eventually persuade, their more immediate task is, through skillful framing, to leave their opponents without access to the rhetorical materials needed to craft a socially sustainable rebuttal. Rhetorical coercion occurs when this strategy proves successful: when the claimant's opponents have been

talked into a corner, compelled to endorse a stance they would otherwise reject" (ibid.: 36). Here, 'talking into a corner' in the context of Snowden's disclosures as well as his media tour, can be understood as a way of highlighting not only the contradictions that arise by way of the United States' self-image, but as an attempt to pressure the United States to confront the issue of widespread surveillance practices in cyberspace in Snowden's terms, "…not by persuading one's opponents of the rectitude of one's stance, but by denying them the rhetorical materials out of which to craft a socially sustainable rebuttal" (Krebs and Jackson 2007: 42). By co-opting the imagery used by state agents, as well as framing the issue in terms of what the United States seemingly values by way of self-image, Snowden creates a moment that must be addressed by state agents at the highest level, whether successfully or unsuccessfully. In doing so, Snowden represents a form of resistance in and through cyberspace by challenging how the state, and its constituents, conceive of the state.

The Snowden leaks and the official response on cyberspace and the leaks following the disclosures can be seen similarly to, say, the Cold War "…as another episode in the ongoing production and reproduction of American identity through the practices of foreign policy, rather than simply an externally induced crisis" (Campbell 1998: 132). While the Snowden leaks represent an aesthetic irruption of state self-identity and self-image with regards to cyberspace, the event itself must be situated within broader state behavior in the digital age. The NSA leaks by Snowden represent a form of counterpower that came about through information disseminated on the internet, and put pressure on an administration, an organization within the state, and the state itself. This moment is fleeting, and represents only a micropressure to traditional notions of state power. However, it is a prime example of a broader ontological insecurity that states must face in cyberspace by virtue of the very characteristics that make cyberspace unique and

attractive for states, at least partially. This ontological insecurity is met with a variety of narratives that seek to dislodge and delegitimize the source of the challenge to security of self.[38] All of this returns to the initial premise of this chapter, that there are a series of contradictions to self-image that the state must mediate in order to "save face" and to justify particular practices in cyberspace. The Snowden leaks, and his presentation at SXSW represent a challenge to that justification and focus attention on the contradictions themselves. As shown earlier, the state attempts to deal with such contradictions through various narratives of American exceptionalism, ahistorical references, a plea to seemingly shared American values, and deflection of responsibility.

viii. Capturing, Co-opting, or Erasing Snowden? Handling the Aesthetic Irruption

Aesthetic irruptions, in the wider scheme of state security, are fleeting moments. While cyberspace poses consistent ontological insecurity for states, aesthetic irruptions that take hold of the imagination for some, for a moment. Thus, what is important when examining the Snowden leaks through the state's response is how narratives change, or how narratives mediate broader concerns about cyberspace in light of such aesthetic irruptions. Debrix (2006: 787-788), in an analysis of Cindy Sheehan's demonstrations outside the Bush farm in 2005, argues that "events as surprises" that take place in the global media can be captured, co-opted, or erased: "But it is nonetheless an event that commands a presence, that does not want to be ignored (in fact, it is its main point), and that brings a haunting reality back in the face of those who promote and champion a higher idea, ideal, and ideology." Steele (2010: 49) notes that counterpower ends when it is quarantined or "classified." Confronting the leaks, official discourse places emphasis on the act of disclosing, rather than the disclosures themselves. Further, when pressured into a

[38] This is not to say that Snowden did the "right" thing; rather, the narratives that circulate that suggest such a thing must be discredited.

response, state response must place the leaks within a broader context that harkens back to state self-identity and self-image, all the while arguing that the behaviors that spurned the leaks are not as problematic as once thought:

> What I did not do is stop these programs wholesale, not only because I felt that they made us more secure, but also because nothing in that initial review and nothing that I have learned since indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens. (President Obama, 17 January 2014 speech on NSA Reforms)

The impact of global media, the 24/7 spotlight on states, and the manner in which the NSA leaks are continually being leaked, places a different sort of pressure on the state than a demonstration that has a clear beginning and end. The magnitude of the leaks leaves too much to be erased. However, the leaks can be captured and co-opted by way of paralleling reforms to self-image, on the one hand, and equivocating these surveillance practices as part of a necessary, and fruitful, security venture on the other (eg. these ventures stopped four security threats from happening). Therefore, while continually harkening back to an idealized image of state self-identity, the Snowden leaks, as aesthetic irruption, are mediated in the same way that the broader contradictions between liberty and security in cyberspace are: through a call to principles that makeup self-identity, calls to security that seize upon public anxiety over cyberspace, and claims of American exceptionalism that suggests that governance in the digital age should be met head on by the United States.

Chapter 5: Conclusion

Through an understanding of ontological security and power as aesthetic, this thesis has attempted to explain how states, particularly the United States, come to understand cyberspace, how cyberspace poses aesthetic challenges to state self-identity, and how states mediate the contradictions that arise in the justification for state intrusion into cyberspace. Born out of a desire to push analysis beyond material conceptions of power and state behavior as strictly survival-based, the notion of ontological security and power as aesthetic guides analysis to the fissures of contradiction in the discourse surrounding cyberspace. Given the recent NSA leaks by Edward Snowden, the United States has had to respond to a series of allegations that run counter to U.S. self-identity and self-image. A country based on Enlightenment-era liberalism—freedom, individualism, private property—has been confronted by state behavior that seemingly runs counter to this self-identity. Underlying this aesthetic irruption—one of state surveillance—lies broader state insecurity about cyberspace. Certainly, part of this state insecurity can be related back to post-9/11 paranoia about issues of terrorism and preemptive prevention of such an event happening again. However, this justification is a façade. President Obama's speech on NSA reforms demonstrates this: underneath a layer of justification for surveillance in general, President Obama's, and the state's, problem seems to be with cyberspace itself. Given James Clapper's statements that cyber terrorism and cyber espionage has supplanted terrorism as the largest threat to U.S. national security, analysis that boils state behavior down to these kinds of state security concerns in cyberspace stops short of full explanatory power. Just as ontological security can help explain, for example, state foreign policy behavior that runs counter to "common sense" strategy, the theoretical framework of ontological security can help explain the contradictions in state discourse and behavior in cyberspace. Further, ontological security and

power as aesthetic is not just about explaining the tension between soft-power and hard-power, liberty and security, etc.; ontological security starts on a different assumption altogether, that states are more than just survival-seeking entities—states seek to affirm their self-identity and self-image.

Ontological security in cyberspace presents a new way in which scholars of international relations can examine state security in the digital age. While traditional assumptions that international relations scholarship has still hold in the digital age, new dynamics by way of cyberspace arise; state self-image and identity in relation to cyberspace demonstrate the importance in international relations scholarship to new forms of state digital power to reconfigure, shape, and reinforce state identity and self-image. Power, here, does not have to take the form of cyber-strike capability, surveillance practices, or cybersecurity. Rather, practices of power are manifest in the ways states attempt to reaffirm, control, and shape cyberspace as well as state self-image and identity. This leaves international relations scholarship with new sets of puzzles in terms of inter-state interaction in the digital age, the particular nature of each state in relation to cyberspace, and the nature of state identity going forward as the world becomes ever more interconnected, interdependent, and reliant on securing information. Ways of conceptualizing the security/liberty contradiction in cyberspace are also important as states attempt to 'reign in' cyberspace to control information flows and state security. Universal values are perhaps nonexistent in a necessarily global arena. Thus, states are left to understand and encounter cyberspace in the terms that the state finds most important. Most of the time, these conceptions of cyberspace attempt to mirror state self-identity (in the case of the United States, liberty, privacy, etc.), and also security.

As President Obama notes, the digital age is in its infancy. Therefore, the insecurities that face nation-states today, by way of physical insecurity or ontological insecurity, will need to continue to be mediated in the future, perhaps to a larger degree. The United States is an interesting case; building from Campbell (1992), the United States is particularly vulnerable to alterations of self-image and thus self-identity. What happens when a land, built upon an absence rather than a presence, is suddenly exposed by contradictions to self-image and self-identity? This is not to say that this is a strictly American phenomenon, but the development of cyberspace, the birth of the U.S. as a nation, and the position of the United States in terms of global power make the United States an example par excellence for state ontological security in cyberspace.[39] Nazli Choucri (2012: 5) notes, international relations theory"…has yet to recognize the implications of cyberspace for the conduct of international relations…" This call can be answered in a plethora of ways. This project has sought to bring to light an understanding of how the state understands cyberspace by way of official state discourse and an example of an aesthetic irruption of state self-image. The contradictions that have been highlighted in this project are at the very heart of contradictions that lead to ontological insecurity: self-image (cyberspace should be like we are, open and free) versus behavior (cyberspace must be secured). However, it goes beyond security, broadly speaking; the NSA leaks paint a picture of state behavior that has been circulated in the global media as dystopic and as a global problem. In other words, the aesthetic irruption problematized state self-image of two distinct groups to the state: its own people, and the international community. Other states, as they responded to the allegations, were not quick to draw focus to their own surveillance practices. Rather, they acted to deflect attention back toward the United States. In turn, as demonstrated by President Obama,

[39] The notion of the "birth" of a nation only exemplifies the state as person in international relations

the United States quickly made reference to who the United States was not (China and Russia) in order to preserve a self-image that is conceived to be in opposition to said states.

While cyberspace has been put at the top of many policy agendas, and the NSA leaks have forced the United States to introduce reforms to NSA surveillance programs, cyberspace is still a privileged space. As Choucri (2012: 53) notes: "In 1999, the United Nations Development Programme (UNDP) argued that the Internet "runs along the fault lines of national societies, dividing educated from illiterate, men from women, rich from poor, young from old, urban from rural."[40] While this still rings true today, World Bank Development Indicators project an increase of internet users from close to two billion in 2010 to 4.5 billion by 2020 (Choucri 2012: 70). As such, what is to come in the digital age is unknown, and, in my view, an increase in participation globally in cyber-related activities, and advancements in technology along the way, can only heighten state insecurity about and in cyberspace. However, here, by way of conclusion, some deference should be made to those who live outside, or tangentially to, cyberspace. As Toal (1999: 150) rightly notes, ""Borderless world" discourses are the fantasies of the few that can dream of becoming digital in a world where just being is a persistent struggle for so many."

Future research might analyze ontological security through analyses of speed more generally in international relations, the transcendence of geography and physicality, and of different ways that cyberspace can pose "threats" to states (lack of attribution in cyberspace, open participation, and lack of accountability).[41] Ontological insecurity, originally conceived, dealt with individuals. As such, future research may look at the ontological insecurity of individuals in cyberspace, or the ontological insecurity of groups in cyberspace (Giddens 1990). Further, analysis of state ontological insecurity can be analyzed through different kinds of

[40] Choucri (2012: 53)
[41] See Choucri (2012: 4)

foreign policies of the internet, ranging from 'digital diplomacy' to global internet governance (or lack thereof): how does digital diplomacy reinforce state image, given the dynamics and problematics related to cyberspace analyzed in this thesis? Further, this thesis focused primarily on the United States and its relationship to cyberspace. The practices of the United States vis-à-vis cyberspace are different, as President Obama noted, than that of Russia or China. Why? Censorship can be understood in terms of a state's attempt to control access to information. Ultimately, this behavior goes beyond any claims that the censorship protects the people—it ultimately protects the state's self-image.

Bibliography

Barnett, M. and Duvall, R. (2005). 'Power in International Politics' *International Organization*. 59 (1): 39-75.

BBC. (2013, December 16). *Profile: Edward Snowden*. Retrieved from http://www.bbc.com/news/world-us-canada-22837100

BBC. (2014, January 17). *Edward Snowden: Leaks that Exposed US Spy Programme.* Retrieved from http://www.bbc.com/news/world-us-canada-23123964

Bell, D. (1975). 'The End of American Exceptionalism' *The Public Interest*, 41: 193-224.

Campbell, D. (1992). *Writing Security: United States Foreign Policy and the Politics of Identity.* Minneapolis: University of Minnesota Press.

Campbell, D. (2003). 'Cultural Governance and Pictorial Resistance: Reflections on the Imaging of War' *Review of International Studies*, 29: 57-73.

Castells, M. (2007). 'Communication, Power and Counter-power in the Network Society' *International Journal of Communication*, 1: 238-266.

Cavelty, M. D. (2013). 'From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse' *International Studies Review*, 15: 105-122.

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge: The MIT Press.

Clarke, R. (2010). *Cyber War: The Next Threat to National Security and What to do About It.* New York: HarperCollins

Croft, S. (2012). 'Constructing Ontological Insecurity: The Insecuritization of Britain's Muslims' *Contemporary Security Policy*. 33 (2): 219-235.

Debrix, F. (2006). 'The Sublime Spectatorship of War: The Erasure of the Event in America's Politics of Terror and Aesthetics of Violence' *Millennium: Journal of International Studies*. 34: 767-792.

Der Derian, J. (1990). 'The (S)pace of International Relations: Simulation, Surveillance and Speed' *International Studies Quarterly.* 34: 295-310.

Doty, R. (1993). 'Foreign Policy As Social Construction: A Post-Positivist Analysis of U.S. Counterinsurgency Policy in the Philippines' *International Studies Quarterly*. 37: 297-320.

Economist (2010). *Cyberwar: War in the Fifth Domain*. Retrieved from http://www.economist.com/node/16478792

Fairclough, N. (1992). *Discourse and Social Change*. Cambridge: Polity Press.

Ferguson, K. (1987). 'Male-Ordered Politics: Feminism and Political Science' in *Idioms of Inquiry: Critique and Renewal in Political Science* (T. Ball, ed.). Albany: State University of New York Press.

Gee, J. P. (1996). *Social Linguistics and Literacies.: Ideology in Discourse*. London: Taylor and Francis.

Giddens, A. (1990). *Modernity and Self-Identity*. Cambridge: Polity.

Gould, H. and Steele, B. (2014) Interview with Rossone de Paula, F., Lawrence, J., Morris, K. *SPECTRA.* 3 (1): 64-92.

Hansen, L. (2006). *Security as Practice: Discourse Analysis and the Bosnian War*. New York: Routledge.

Hansen, L. (2011). 'Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis' *European Journal of International Relations* 17 (1): 51-74.

Harvey, D. (1989). *The Condition of Postmodernity.* Oxford: Blackwell.

Hodges, A. (2011). *The "War on Terror" Narrative: Discourse and Intertextuality in the Construction and Contestation of Sociopolitical Reality*. New York: Oxford University Press.

Kinnvall, C. (2004). 'Globalization and Religious Nationalism: Self, Identity, and the Search for Ontological Security' *Political Psychology*, 25 (5): 741-767.

Kramer, F. (2009). 'Cyberpower and National Security: Policy Recommendations for a Strategic Framework' in *Cyberpower and National Security* (F. Kramer, S. Starr, and L. Wentz, eds.). Dulles: NDU Press.

Kuehl, D. (2009). From Cyberspace to Cyberpower: Defining the Problem. In Kramer, K., Starr, S. & Wentz, L. (Eds.), *Cyberpower and National Security*. Dulles: Potomac Books.

McCarthy, D. (2011). 'Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet' *Foreign Policy Analysis*, 7: 89-111.

Milliken, J. (1999). 'The Study of Discourse in International Relations: A Critique of Research and Methods' *European Journal of International Relations*, 5 (2): 225-254.

Mitzen, J. (2006). 'Ontological Security in World Politics: State Identity and the Security Dilemma' *European Journal of International Relations*, 12 (3): 341-370.

Singer, P. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford University Press.

Steele, B. (2008). *Ontological Security in International Relations: Self-Identity and the IR State*. New York: Routledge.

Steele, B. (2010). *Defacing Power: The Aesthetics of Insecurity in Global Politics*. Ann Arbor: University of Michigan Press.

The White House. (2009). *Cyberspace Policy Review*. Retrieved from http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

The White House. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Toal, G. (1999). 'Borderless Worlds: Problematizing Discourses of Deterritorialization.' *Geopolitics*, 4: 139-150.

Weldes, J. (1999). *Constructing National Interests: The United States and the Cuban Missile Crisis*. Minneapolis: University of Minnesota Press.

Wendt, A. (2004). 'The State as Person in International Theory' *Review of International Studies*. 30: 289-316.

Zarakol, A. (2010). 'Ontological Insecurity and State Denial of Historical Crimes: Turkey and Japan' *International Relations*, 24 (1): 3-23.