ABSTRACT

OSWALD, KATHLEEN FRAZER. Smarter, Better, Faster, Stronger: The Informationalized Infrastructural Ideal. (Under the direction of Dr. Jeremy Packer).

As the public and private sector spend and invest billions of dollars maintaining, repairing, securing, constructing, and informationalizing infrastructure, scholars of communication continue to neglect the central role of infrastructure in shaping contemporary mediascapes. This neglect stems from a number of tendencies in the field of communication, including a move away from the transmission model of communication, a separation in thinking about the communication of information and the communication of people and objects, and a tendency to think about technologies in terms of their historical development, mediation, effects, uses or potentials rather than to understand technologies as cultural forms subject to alternative arrangements. While these academic biases make the study of communication, mobility, and technology challenging, my work takes an interdisciplinary approach that recognizes and works to move past historical divisions in the disciplines in the interest of exploring the ways in which informationalization is changing communication, culture, and mediascapes.

I locate informationalization—adding a data layer to processes through instrumentation, interconnection and intelligence—at the center of changing articulations of communication, transportation, information and housing infrastructure. I take as central a double reorganization of infrastructure under two competing logics: a utopian view that positions the informationalization of networks as "smart" and can be traced across a variety of popular, industry and government discourses as a compelling argument for connection; and a logic that positions infrastructure as "critical," which while intensified by post 9/11

sensibilities, has clear origins in earlier beliefs about the dystopian potentials of connection, including computer crime and cyberwarfare. I first develop a set of working definitions for a variety of terms as they relate to informationalization. I then explore specific contexts of informationalization, examining utopian discourses of connection as "smart" in a growing market for electrically powered automobility, dystopian discourses of informationalization in terms of critical infrastructure and cyberwar, and finally to disconnection, examining the grid and "grid away from the grid" life assurance solutions. Through these cases, I work to understand informationalization as an apparatus that rearticulates infrastructure according to a new infrastructural ideal and an associated politics of security that are coextensive with both utopian and dystopian discourses of informationalization.

I ultimately argue that communication and mobilities scholars must look to processes of informationalization with a particular emphasis on those infrastructures that are designated both "smart" and "critical" in order to reveal the ways in which smart infrastructure can mean more than informationalized infrastructure, and to discern to what and to whom critical infrastructure is critical. It is my hope that this project will serve as a starting point for productive and meaningful interdisciplinary collaboration concerning a process that promises to radically alter the way that we access and use communication, transportation, housing, services and infrastructures.

Smarter, Better, Faster, Stronger: The Informationalized Infrastructural Ideal

by
Kathleen Frazer Oswald

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Communication, Rhetoric, & Digital Media

Raleigh, North Carolina

2011

APPROVED BY:

_____	_____
Jeremy Packer, Ph.D. Chair of Advisory Committee	Stephen B. Crofts Wiley, Ph.D.
_____	_____
Melissa Johnson, Ph.D.	Rebecca Walsh, Ph.D.

DEDICATION

To Jordan, my Best Friend

This would not have been possible without your love and support.

And Mom and Dad

Who never stopped believing in me.

BIOGRAPHY

Kathleen Frazer Oswald is a communication scholar with research areas in communication technology, communication policy and regulation, and mobilities studies. Her dissertation looks to the informationalization of infrastructure with a particular focus on smart and critical infrastructure, arguing that an examination of the cultural implications of informationalization is critical in developing an understanding of mediascapes, mobilities, and communication. She has co-published two pieces with her dissertation adviser Dr. Jeremy Packer on mobile communication technologies and the work of Raymond Williams. Before coming to North Carolina State University to pursue a PhD in Communication, Rhetoric, and Digital Media, she completed an M.A. in Communication at Villanova University, defending a thesis titled "Hacking subject, subjecting hacking: Crisis in technoculture" (2006) under the direction of Gordon Coonfield. Prior to her graduate studies, Oswald attended West Chester University in her hometown of West Chester, PA, graduating with a B.A. in Communication Studies (and a minor in Latin) in 2004.

Oswald has presented at regional, national, and international conferences on topics that range from broadband as social space to cyberwarfare, and teaches courses in communication law, critical analysis of media, public relations and organizational communication. Prior to teaching, she worked in the field of public relations as an account executive serving clients in a range of industries from biotech to manufacturing, and also at West Chester University as a PR Coordinator. She was Board Secretary and Lead PR Volunteer at Chester County InterLink (ccil.org), one of the first (and last remaining) freenets in the country.

AKNOWLEDGEMENTS

Throughout the course of this project, I have learned that one does not simply write a dissertation: one rather goes on a journey through knowledge with mentors, colleagues, friends and family that results in a new way of thinking about things. Here I would like to acknowledge those who have made this journey possible.

I would first like to thank my committee for supporting my research at the intersection of communication, technology, and mobility. In addition to chairing my dissertation committee, Jeremy Packer has been a great teacher and mentor: the two pieces that we co-authored have gone a long way toward helping me find my confidence as a scholar, and for that I am deeply appreciative. Melissa Johnson's focus on definitional work has helped me to find the words I needed to start a conversation about informationalization and infrastructure. Rebecca Walsh provided an outside perspective that served as a constant reminder that this project had relevance across disciplines. The early and constant encouragement of Steve Wiley was instrumental in this project: without it, this dissertation would likely have been about something else. Steve's thoughtful feedback has always challenged me to think in broader terms, and I am a better scholar for it. I could not have asked for a better committee. Thank you all for your feedback, encouragement, and support.

Shayne Pepper, Ruffin Bailey, Nathaniel Poor, Kate Maddalena and Kathy Oswald Sr.; there are many words that make up a dissertation, and you have helped me to make sure I am using the right ones. Your proofreading support has been a major part of making this dissertation a reality.

I am indebted to the students and faculty who have made North Carolina State University a place I am proud to call home. Victoria Gallagher and Carolyn R. Miller, thank you for all of your hard work founding the CRDM program; I cannot imagine what my life would be like if I had gone anywhere else. Deanna Dannels and Susan Miller-Cochran, you have prepared me to be the best teacher I can be. To my students: the opportunity to teach has been a gift, and I thank you for the opportunity to learn together.

To my cohort and classmates: thank you for helping to make seminars productive thinking spaces. To all of my CRDM colleagues: though we have not all had classes together, I have become friends with many of you and am proud to count myself among you – an impressive bunch! A special thanks to CRDM Alumni Christian Casper and Anna Turnage who have been great sources of advice and inspiration. Dan Sutko, Jordan Frith, Seth Mulliken and Fernanda Duarte, I look forward to working with you in the years to come as our paths intersect in mobilities studies. NCSU Masters alumni Adam Richard Rottinghaus, Dan Kim, and Kevin Flannigan deserve special mention for intense theoretical discussions and ridiculously good times; you will always be Wolfpack to me!

I also want to acknowledge my professors at Villanova University—particularly my M.A. adviser Gordon Coonfield and committee members Bryan Crable and Maurice Hall—who were instrumental in helping me to discover that I had a home in academia: I am forever indebted to you. I also want to thank Villanova M.A. alumni with whom I have had great conversations about communication, technology, space, and other fantastic things—George Boone, Brett Lyszak, and Nathan Taylor—may our paths continue to cross.

A number of friends and colleagues have been especially important to me during my time in North Carolina. Dawn Shepherd, you are a better friend than I could have imagined making when I set off for Raleigh. Shayne Pepper, you are a fixed point in chaotic times. Kelly Norris Martin, you are a ray of sunshine, and never fail to make me smile! Ruffin Bailey, writing with you has changed me forever (in a good way), and our conversations have been extremely helpful. Nick and Nicky Temple, Mark Christensen, Jason Richardson, James Burka and Kevin Brock, you have taught me that I always have time for fun and games and food, no matter how busy I am. You have been like a family away from home.

My family has been an amazing source of strength and support throughout my academic pursuits. Mom and Dad, thank you for making me go to college in the first place, and, when it went way further than any of us expected, for giving me the strength to keep going. Thomas, having you as a brother has made me a better teacher (sorry about the homework I used to invent for you in the summer… I was destined to teach). Poppie, thank you for the weekend road adventures that prepared me for the travel this line of work demands. G-mom, from the beginning you taught me to look for beauty in everyday things: what I have been doing all these years is exactly that, so thank you for teaching me to look somewhere non-obvious for something amazing. Pieter Raams, thank you for your support and friendship over the years. To my in-laws—"Other Mother," Gram, Pop and Shari—no one could ask for a more supportive bonus family, and thank you for letting me take Jordan to North Carolina for four years!

Jordan Laster, you are my best friend and an amazing husband. Thank you for more than I have the words to say. You bring out the best in me, and this journey would not have been possible without you. I look forward to what life brings us next. I love you.

TABLE OF CONTENTS

LIST OF FIGURES

Introduction

Underground, undersea, overland and in orbit are vast assemblages of infrastructure enabling the movement of data, goods and bodies in today's digitally networked environment. As the electric grid becomes the smart grid, electric vehicle infrastructures are built out, and telecom companies extend "fiber to the door" service, our various grids are more tightly coupled through informationalization. While processes of informationalization, or adding information layers to infrastructures, systems, and processes, make life increasingly 'convenient,' they also make systems more vulnerable to failure and attack, necessitating upgrades in bandwidth, redundancy, and security.

IBM's "Smarter Planet" campaign asks the viewer to imagine a world made better through a seemingly simple three-step process that will occur across systems, sectors and spaces: "1. Instrument the world's systems; 2. Interconnect them; and 3. Make them intelligent" (IBM, 2011b). Across IBM's website, reports, presentations, case studies and conversations argue that informationalization will help companies get better returns on investments and help governments provide better education services, make cities and transportation systems safer, and improve operations. The site explains that as ever more data is collected on everything from technological and natural systems and processes to the attitudes of consumers, citizens and students, "…data by itself isn't useful. The most important aspect of smarter systems is the actionable insights that data can reveal" (IBM, 2011a). What is crucial is being able to turn this data into information by making it actionable, and in so doing, making the world smarter one system at a time. In IBM's vision of making the world a better place, informationalization is the driving process.

In "From Windscreen to Widescreen: Screening Technologies and Mobile Communication" (2010), Jeremy Packer and I discussed processes of mediated informationalization as contributing to the role of information technologies in presenting users with a world that is increasingly accessible to subjects via *screening technologies* or those technologies that, for better or worse, have come to be a primary access point to the ways in which information is gathered, processed, and acted upon. We explain that mobile screens work to informationalize experience, "screen[ing] out noise to heighten clarity, allowing specific forms of knowledge to form that dictate what matters for any given situation" sorting data to produce "relevant" information for users and govern mobile conduct (2010, p. 316). This conduct is not only governed at the level of the user, but also within the systems and infrastructures that are becoming informationalized—or made "smart"—through the addition of increasingly dense and extensive information layers. In this project, I am interested primarily in the impacts of informationalization at the level of infrastructure, as the addition of information to processes reorganizes the ways in which myriad communication, transportation, economic and political exchanges are carried out.

To further explore the informationalization of infrastructure, I look at both the processes and the possibilities of informationalization across a number of sites. In chapter one, I define a series of key terms that will serve to clarify the work moving forward, including infrastructure, network, system, informationalization and smart. Chapter two provides a history of the foundations of an emerging electrically powered automobility system with a particular focus on the ways in which electric automobility has been made smart through informationalized infrastructure, looking to the Better Place electric automobility platform as a case study. The third chapter focuses on dystopian aspects of

informationalization, namely in the context of infrastructure as target, examining the role of critical infrastructure in both military strategy and homeland security. This chapter takes the Stuxnet worm that targeted industrial processes at a uranium enrichment facility in Iran as a case that not only proves that cyber-mediated warfare is effective, but also legitimates efforts to secure critical infrastructure in the United States. Chapter four focuses on logics of disconnection and immobility through an examination of bunkers and shelters from the Cold War to the present and sees shelter space as an infrastructure of survival for the "smart subject." This introduction begins with an examination of some of the challenges in studying these topics from a communication perspective, situates this project among other approaches, maps the approach of this project and summarizes the chapters to follow in more detail.

As the public and private sectors spend and invest billions of dollars maintaining, repairing, securing, constructing, and informationalizing infrastructure, scholars of communication continue to neglect the fundamental role of infrastructure and logics behind the reorganization systems, institutions, and practices. This neglect stems from a number of tendencies in the field of communication, including a move away from the transmission model of communication, a separation in thinking about the communication of information and the communication of people and objects (transportation), and a tendency to think about technology in terms of their historical development, mediation, effects, uses or potentials rather than to understand technologies as cultural forms subject to alternative arrangements. While entrenched academic traditions make the study of communication, mobility, and technology challenging, my work takes an interdisciplinary approach that recognizes and works to move past historical divisions in the disciplines in the interest of exploring the ways in which informationalization is changing communication, culture, and mediascapes.

While moves away from the cybernetic tradition in the field of communication opened up new areas for exploring the important role of communication in a variety of cultural contexts, there is a need to study the ways in which significant changes at the level of transmission are affecting the practice of communication. Cybernetics, a tradition which looks to the transmission of signals and feedback loops in both technological and nervous systems, stemmed from early work in engineering that sought to explore and understand rudimentary electric communication technologies. James Carey argues in "A cultural approach to communication" (originally appearing in the journal *Communication* in 1975 and reprinted as chapter one of *Communication as Culture*, 1989) that a transmission view of communication based on mathematician Norbert Wiener's *Cybernetics* (1965)—one that focused on the reproduction of a signal across distance—was too spatial, and that communication must also be thought of in terms of a ritual view. Carey explains that "a ritual view of communication is directed not toward the extension of messages in space but toward the maintenance of society in time; not in the act of imparting information but the representation of shared beliefs" (p. 18).

Jansson and Falkheimer draw on Carey's distinction between transmission and ritual communication, arguing that the transmission view of communication is not suited for analyzing the ephemeral media of the present, while the ritual view does not account for the spatial ambiguities that communication produces and is too critical of a space-based view of communication (2006, p. 15). They suggest that the spatial turn in media studies moves beyond this dichotomy by ideological and political, technological, and textural dimensions that focus on the ways culture is materialized through communication and transportation, providing a way to rethink communication more productively.

At present, engineers, urban planners, government officials, and multi-national corporations are working to implement programs to informationalize communication, transportation, and utilities infrastructures. At this time, communication scholars must be attentive to the ways in which these processes are tied up in larger cultural, political, economic and social issues. Communication as a field is uniquely suited to explore such connections, particularly due to its already interdisciplinary nature, which encompasses issues of communication at a variety of scales (interpersonal to mass), historical foci (from early symbol use to digital media), media (unmediated to hypermediated), and approaches (social scientific to rhetorical analysis and cultural studies). To understand the ways in which the mediascape is changing, re-focusing on the role of transmission in communication is critical. As informationalization facilitates a "Smarter Planet" where infrastructure, government, industry, and communities converge with information systems, who is best suited for understanding these changes if not communication and critical cultural scholars?

The divide in thinking between communication and transportation poses a challenge to such analysis, though there is much evidence to suggest that the field of communication is increasingly accepting that the study of mobility is an important piece in understanding communication more broadly, particularly as next-generation mobile devices untether communication from fixed spaces and make communication possible wherever a person, a device, and bandwidth are co-located. A body of work around Raymond Williams' notion of *mobile privatization* has long looked at the intersection of communication, mobility and technology (Hay, 2001, 2006; Hay & Packer, 2004; Packer, 2002; Spigel, 2001), and work focusing on the materiality of communication also tends to incorporate mobile aspects of communication. North Carolina State University's fall 2009 symposium, "Materializing

Communication and Rhetoric: Technologies, Infrastructures, Flows" and the subsequent edited collection *Communication Matters: Materialist Approaches to Media, Mobility, and Networks* (Packer and Wiley, 2011) points to such increased focus on the materiality of communication, paying specific attention to the role of technology, mobility, infrastructure, policy and practice in understanding a dynamic media environment and demands new approaches that range from social scientific to rhetorical, spatial and cultural critical. Wiley, Sutko, and Moreno (2010; 2011) have explored the material communication and transportation practices of individuals through ethnographic work, illuminating subject perceptions of social space and bringing a needed material and spatial element to social network analysis such as Wellman's "small world" studies. Work in the emerging fields of the geography of communication and mobilities studies has also underlined the need to examine material practices at the junction of communication, transportation and technology from a range of disciplinary perspectives including communication, geography, and sociology (Packer, 2002, 2006, 2008; de Souza e Silva & Frith, 2010; Cowen, 2009, 2011; Graham, 2009, 2010; Jansson & Falkheimer, 2006; Urry, 2003, 2007; Sheller, 2007). To begin to get at the important ways that informationalization is changing communication, mobility and culture, more work that accounts for the critical link between such technologies and practices is necessary.

The work of Harold Innis (1951/2008) and James Carey (1989) demonstrates the value of approaches that look to the intersection of communication and mobility. Innis' observation of space- and time-biased communication demonstrated a clear connection between the materials and forms of communication and transportation technology on the growth of civilizations. James Carey's work on the telegraph and the train in working to

solidify the populace of the United States during a time of westward expansion (as well as the role of the telegraph in managing the train) further established a connection between communication and transportation technologies. Drawing on Carey's work on the relation between the train and the telegraph in "Technology and Ideology" (1989), Packer (2006) analyzes a series of communication and transportation pairings, including the relation between seafaring, air travel, and automobility with radio in order to demonstrate the ways in which communication and transportation technologies have been brought together to increase safety and surveillance of mobility. Packer argues that while "[c]ommunication technologies may not have been dependent upon transportation technologies for more than 150 years," the connections between the two are of great importance particularly in terms of the way that communication technologies are leveraged to exercise control at a distance and to make mobility safe (2006, p. 81). Calling for a rethinking of the relation between transportation and communication technologies, he argues that the "split in our thinking about communication and transportation has left a hole in our field" that would be "covered" by a variety of other interests (2006, p. 94). Focusing largely on the ways in which communication and transportation have been brought together to make populations safe, he takes a Foucauldian perspective to explore culture, communication and transportation technologies such as automobility and the CB radio (2002), the Segway (with Hay, 2004), motorcycles and hitchhiking (2008), and the Hummer (2007). In recent co-authored work, Packer and I have examined the relation between the automobile and mobile devices, paying particular attention to the ways that the automobile has served as a test bed for mobile communication technologies such as portable music players and cellular phones (2010).

A final major challenge I associate with trends in thought about communication is a tendency for technologies to be considered as objects of study rather than practices and processes that express broader logics of social, economic, and political relations. Such thinking often threatens to fall into common traps of either technological determinism, where it is imagined that a particular technology dictates that humans behave with it in a particular way, or cultural determinism, which removes all agency from the technology itself, arguing instead that humans came to construct a technological object or a collection of technological objects in a particular way based on a cultural need. An academic exemplar that escapes this binary is Raymond Williams' approach in *Television: Technology and Cultural Form* (1974, 2003), which looks at television as a *cultural technology* that interacts with and makes possible a variety of *cultural forms.* Williams explains that while some have discussed television in terms of the ways in which it incorporated elements of antecedent technologies, it is also important to consider new cultural forms made possible by television, including television itself; he observes that "there are moments in many kinds of programme when we can find ourselves looking in what seem quite new ways…. What can then happen, in some surprising ways, is an experience of visual mobility, of contrast of angle, of variation of focus, which is often very beautiful" (1974, 2003, p. 75). In exploring informationalization as a cultural technology that takes a variety of cultural forms, we must understand not only the ways that informationalization remediates cultural forms such as the electric grid, automobility, war and notions of survival, but also what informationalization as a cultural form looks like: what makes it significant? What does it change about communication and how it should be understood? How does its operation at the basic level of infrastructure change the ways that the world is lived, experienced and communicated?

Importantly, the work of informationalization is taking place at the level of infrastructure (where instrumentation makes the collection of data possible), and so to explore this particular cultural form, we must first render infrastructure sensible. This means not only calling attention to its existence, but also understanding how new configurations of information, technology and security change the ways that we make sense of the world. This work entails more than a history of infrastructure, an analysis of the material composition of networks, or a review of the policies and regulations that shape their development, deployment and maintenance. Requiring vast investments of time, money and physical labor, infrastructure deployments become heavily invested in particular directions leading to, quite literally, sunk-costs (when you travel five miles in one direction, you cannot "untravel" them – you have already made the investment). Identifying the logics driving the development of these systems (rather than merely their histories) will enable us to better understand what actions and activities systems are designed to enable and constrain, how moves to make infrastructure "smart" through processes of informationalization change these configurations, and what set of concerns, ideas and agendas influenced development in one way and not another.

While geographer John Urry frames infrastructures as systems of immobility, my work sees infrastructures as dynamic spaces of movement, force, and power relations. To think about infrastructure in terms of simply where it is and is not is to see infrastructure as a static image; no more than a *tracing*. Deleuze and Guattari's *Capitalism and Schizophrenia: A Thousand Plateaus* (1987) challenges us to make maps rather than tracings, explaining that the tracing follows from a tree-like logic of reproduction:

> Its goal is to describe a de facto state, to maintain balance in intersubjective relations, or to explore an unconscious that is already there from the start, lurking in the dark recesses of memory and language. It consists of tracing, on the basis of an overcoding structure or supporting axis, something that comes ready-made. The tree articulates and hierarchizes tracings; tracings are like the leaves of a tree. (p. 12)

Though tracings or descriptions of infrastructure could be organized by overcoding structures such as technological progress, invention, or ingenuity in order to be made sensible as part of a longer history of man and machine, that is not my intention here. My intention with this project is to understand the various logics by which infrastructures are made to achieve anticipated and unanticipated outcomes in systems. I am interested in a process of creating a map, which unlike a tracing, "is open and connectable in all of its dimensions; it is detachable, reversible, susceptible to constant modification… it can be drawn on a wall, conceived of as a work of art, constructed as a political action or as a meditation" (p. 12). The story of infrastructure that will be told in this dissertation does not follow a historical trajectory from invention through development to deployment and adoption. It does not celebrate men of genius, early adopters, or cutting-edge design. Instead, this project seeks to understand the ways in which infrastructure is articulated with information with the goal of producing a *map* of infrastructure, one that would enable *intervention* rather than mere representation. The map will focus on infrastructure as means for directing and re-directing material, electrical, informational and social flows, building and supporting cultural foundations and effectuating logics of governance, commerce and social control.

To that end, this research takes as central a double reorganization of the function and structure of networks under two competing logics: first, a utopian view that positions the informationalization of networks as "smart" and can be located across a variety of popular, industry, government discourses as a compelling argument for connection; and second, a

logic that positions infrastructure as "critical," which, while intensified by post 9/11 sensibilities, has clear origins in earlier beliefs about the dystopian potentials of connection, including computer crime and cyberwarfare. While we are perhaps more familiar with the rhetoric of the smart sublime, the underside of connection is perhaps best introduced via the notion of electronic Pearl Harbor or the "fire sale": a three-pronged attack on networked infrastructure designed to immobilize populations, blind military and government, and create an environment of fear in the face of an unknown threat. Despite their apparent conflict, what underlies both logics is the centrality of networked information technology and infrastructure to radically affect (for better or worse) the future of our world.

The overall strategy of this project is to explore the history of the present condition of informationalized infrastructure. To accomplish this, I develop a set of working definitions for a variety of terms that have been used (often loosely) in academic research on infrastructure, government policy, and in the popular press. I then explore utopian and dystopian discourses of informationalization through specific contexts, looking to connection as smart in a growing market for electrically powered automobility and turning later to dystopian discourses in critical infrastructure and cyberwar. Finally, as an alternative to connected infrastructure, I look to those instances where the grid is "off," individuals choose to live "off the grid," and finally examine grid-away-from-the-grid life-assurance solutions and survival shelters (should events in 2012 or beyond threaten the current mainstream model of a connected and informationalized way of life).

A second focus here is the ways in which economy and security play out within these utopian and dystopian frames; these tensions are examined throughout the cases presented in chapters two, three and four. In the conclusion, I discuss the informationalized infrastructural

ideal in more detail. As a site of increasing informationalization, infrastructure has not only become an economic growth area in terms of generating profit in transmission and distribution, but also the object of government funding, technological innovation, military interest and homeland security. One orientation toward infrastructure, connectivity and security can be understood through the notion of the "fire sale," which will be discussed later in more detail. In short, the notion of fire sale at the core of the plot in *Live Free or Die Hard* (2007) and "Electronic Pearl Harbor" (a simulation run by the United States government in the late 1990s) suggests that informationalized infrastructure is vulnerable to attack via information networks. Such attacks could result in multiple cascading failures of multiple critical infrastructures, crippling utility, transportation, and communication capabilities at a national (or global) level. The origins of such scenarios will be discussed later in this project. In the next section, I review some of the literature on the topic of infrastructure and various related technological systems and networks as they have been taken up by scholars in a range of disciplines, focusing on the benefits and disadvantages for understanding informationalized infrastructure via their approaches.

Placing Infrastructure in Other Approaches

This project examines infrastructure in an effort to understand how the very underpinning of systems are being reorganized as "smart" and "critical" through popular, corporate, government and military discourse. As infrastructure is coupled with information technology, the basis for seeing network infrastructures as "smart" systems and as potential sites of cyberattack doubles, and infrastructure becomes an increasingly important topic for communication scholars to explore. While many have looked at the historical development of

various technologies, practices, and systems, (see Hecht, 1999 on fiber optic; Merriman, 2007 on the M1; Hughes, 1983 on electricity) and histories of practice have been considered from cultural studies perspectives (Chun, 2006 on fiber optic, Packer, 2008 on automobility), studies that position infrastructure as central (such as Graham, 2009; Graham, 2005; Graham & Marvin, 2001) are less common. A review of the place of infrastructure in the history of systems, studies of technology and culture, political economy and geography situates the contribution of this project as significant. I will expand and clarify the role of informationalized infrastructure in larger systems, from specific technologies such as "smart metering" of electricity use as critical in the move to a "smart grid," or to think of the "smart grid" as an infrastructural element central to larger systems such as electric mobility.

A number of approaches have been used to explore the history of the development of technological systems. First, communication scholars and historians have focused on system development in order to understand the process by which infrastructure is developed and maintained over time; how its material structure enables and constrains action; and how systems, even when detached from original infrastructures, retain elements from previous forms. One route to achieving this is through the Large Technical Systems (LTS) approach developed by Thomas Hughes in *Networks of Power* (1983). Initially outlined in an analysis of the development of electricity in the United States, this approach looks at the development of systems through a series of phases: 1) innovation and development, defined first by inventor-entrepreneurs and later by "engineers, managers, and financiers"; 2) technology transfer, where systems are taken up in different regions; 3) system growth, or the process of identifying imbalances and critical problems; and 4) momentum, where the involvement of materials, people, and organizations shape the direction and goals of a system and create a

systems' culture (pp. 14-15). Graham & Marvin (2001) argue that this approach provides "rich insights into how groups of innovations become linked together to (sometimes) gain the systemic qualities of networked infrastructures" (p. 211). The LTS approach has also been used by researchers working on an NSF-sponsored project to understand and develop policy for cyberinfrastructure, focusing mainly on the historical development of infrastructure and the use of "gateways, i.e. material or social technologies (e.g. standards and protocols) that permit the linking of heterogeneous systems into networks and internetworks" (Jackson et al 2007, para. 5). The LTS approach is useful in understanding how systems develop to serve particular purposes and in incorporating the concept of "gateways" as a way of thinking about the interlinking of systems points; "gateways," here, are social and material technologies by which systems, over time, can become interlinked and networked with other systems. The use of the term "infrastructure" in this context suggests that while the Internet in fact operates as a system (material elements and protocols organized to achieve the movement of information), this very system constitutes an infrastructure for other systems, thus becoming cyberinfrastructure.

While Hughes' approach focuses on the initial development of large-scale systems, his work does not place the same focus on culture; histories of communication and technology often offer a more detailed understanding of how design decisions were made and technologies were understood and practiced. Some of the more nuanced aspects of systems development, as explored in the work of Susan Douglas (1987) in her work on early radio, Menaham Blondheim (1994) on the development of the Associated Press, and Jeff Hecht (1999) on the development of fiber optic technology, provide insight into the impact of specific actors, technologies, and historical events on the development of systems and

infrastructures. Work in this vein often focuses on a specific system through the historical investigation of practice, policy, and technological development. Histories of communication technology contribute knowledge about the impact of various actors, technological advances and historical events on development and explore how systems came to be historically and culturally significant. Douglas' *Inventing American Broadcasting 1899-1922* (1987) details the development of radio from its initial deployment in the late 1800s as it was portrayed in the popular and trade press through to the early stages of the formation of broadcasting, focusing on the place of the "inventor-hero" in the popular press, the history of technical developments and business partnerships, and responses in technical journals to the development of wireless telegraphy and later radio. In another history of technology, Blondheim's *News over the Wires* (1994) takes up an analysis of the development and impacts of the Associated Press, focusing on people and practices as central to the development of this system. Examining fiber optic technology from early lab experiments through to its incorporation in medical imaging and communication infrastructure, Hecht's *City of Light* (1999) focuses on the materials, people and practices involved. There is some discussion of competing technologies, such as the millimeter waveguide (an alternate trunk communication technology), but the research mainly focuses specifically on the development of fiber optic technology. Works in this tradition come from a variety of disciplines, but they share a similar overall perspective that locates technology in a larger historical context and is both a rich source for developing a history of infrastructure as well as a potential site of analysis of discourses of the technological sublime relating to large-scale infrastructures in the United States.

Infrastructure is also a consideration in political economy and policy, as it is in Manuel Castells' multi-method *Communication in Network Society* (2000), which draws on historical evidence, statistics and case studies to explain "network society." Graham and Marvin (2001) identify his approach as "spatial political economy" (p. 213); Castells examines digital technologies and practices as well as networks of capital, industry, and labor and migration. Strengths of the approach are Castells' focus on not only changing information networks, but also networks of capital, industry, and labor, making broad linkages among changes in an overall shift to informational society. His analysis yields perspective largely on economic relations and issues such as global interdependence, changing organizational logics, and changes in workforces, both in other places and historically. Harold Innis (1951/2008) is perhaps best known in communication for making a distinction between time-binding technologies, which extended cultural power over time, and space-binding technologies, which worked to extend the reach of power over space. Innis' work had its roots in analysis that focused on political economic issues (he wrote his dissertation on trade in Canada), which provided the grounding for his later observations on technology, space and time. Innis focused on the time/space bias of various media such as stone, paper, papyrus and parchment, and made claims about societies based on their use of media as to whether motivation seemed to align more with preservation of culture over time (using media such as stone), or extent and reach over space (as is seen with the use of light media such as paper). Such work examines the foundations of economy and state power as a way of understanding something about infrastructure development, placing it in historical, economic and cultural contexts.

In one particularly detailed example, George R. Taylor's economic history of transportation technology 1815-1860, the *Transportation Revolution* (1951), tells a story about transportation infrastructure development in the developing United States. Through more than 400 pages of detailed history and situated as part of a larger series of books titled "The Economic History of the United States," Taylor focuses on political and cultural constraints of transportation technologies as they relate to economic development. Through this analysis, transportation technology is positioned as a means by which a national economy came to develop, making extended reach over territory possible. What these histories indicate is that infrastructure development in the United States (and as far back as the colonial era) was primarily driven by economic interests: while roads were necessary for the mobilization of troops, what initially spurred the development of transportation, utility and communication infrastructures were economic interests. Even in the case of radio, the origins of which are often tied to the U.S. Navy, it was entrepreneurs who worked to fit Navy fleets with equipment that many captains found unnecessary and bothersome, and a number of them did not even bother to use the equipment (Douglas, 1986).

To summarize, while LTS, cultural historical, economic and historical economic approaches are useful in terms of understanding the context of system development, such histories often tell a story of development as if it were slowly but surely carved into stone. Through the reliance on specific actors and geographical and historical conditions, these stories construct a narrative of linear technological development, tracing the path to the current state of technology rather than mapping present articulations in a way that would demonstrate the potential for infrastructure to be assembled otherwise.

One way to get at the larger set of cultural changes that accompany the informationalization of infrastructure is to explicate the connection between technology and culture by situating technologies themselves as cultural and tied to larger logics affecting both technological and social systems. In *Television* (1974/2003), Raymond Williams situates the emergence of broadcasting in a broader context of changing markets, products, practices and technologies as part of an "operative relationship between a new kind of expanded, mobile and complex society and the development of a modern communications technology" (pp. 12- 13). In tracing the origins of television, Williams describes two phases of communication: an *operational* phase that envisioned the sending and receiving of messages as primarily a military and business technology, and a second phase—*broadcasting*—which he explains was of great import in the development of an emerging mass culture. Situating broadcasting in an expanding market of "consumer durables" such as appliances and automobiles, Williams contrasts public technologies such as street lighting and railways with "a new kind of technology for which no satisfactory name has yet been found" which he explains is a form of "mobile privatization" (p. 19). Mobile privatization, then, refers to a tendency associated with a group of emerging technologies that organized mobility, privacy, technology, communication and the home in new ways. Seeing this tendency, as Packer (2010) suggests, as an *apparatus*: "a strategically organized network of discursive and nondiscursive elements brought together to address problems resulting from specific formations of knowledge" may be the most productive route to understanding how such logics come to organize broader relations between technology and culture. A focus on what kinds of systems are being built with informationalized infrastructure and an identification of what knowledge formations or procedural formations they work to capture is

a main focus of this work, particularly since the same articulations are often intersected by both a "smart" and a "critical" apparatus.

Importantly, Williams' *Television* was not interested in television alone. Rather, the work deals with establishing television as a cultural technology in larger trajectories of capital, mobility and culture as well as a detailed analysis of the programming of *flow*, which indicated a shift from programming in terms of discrete blocks of time and rather considered the experience of watching television from a more fluid and mobile standpoint. Such thinking plays quite well more than 35 years later as time shifting, space shifting and device shifting of what we now more generally refer to as "content," rather than programming, is accessed not only via over-the-air broadcasting, satellite and cable services, but also through physical storage media such as VHS, Laser Disc, DVD and Blu-ray or downloaded as media files to a computer or DVR hard drive, or rather "streamed" through a constant connection to a distant source. The notion of streaming free content (YouTube) or having paid access to a larger database of content or pay-as-you-go cloud (Netflix, iTunes) indicates a continued ability for media to become increasingly mobile, fluid and personal. As Packer and I have argued in a piece focusing on Williams' flow and mobile media, while the notion of flow is still relevant, *on-demand* better describes a new model of flow accomplished through the use of technologies of screening where subjects have content at their fingertips (literally) wherever they are, and are at the same time themselves the content of a larger flow organizing consumption, mobility, and security (Oswald & Packer, 2011).

Scholarship considering communication, technology and mobility is perhaps best captured presently in work following the spatial and mobilities-focused turns in the social sciences, which have resulted in newly formed sub-disciplines including the geography of

communication and mobilities studies. These interdisciplinary fields have drawn interest from scholars in departments that range from communication and geography to civil engineering and sociology as well as from officials in municipal, local, state and national governments. Such work focuses largely on the ways in which users, residents, industry, government, planners, architects and artists produce, manage, live in and move through spaces both real and imagined with a focus on understanding articulations of people, technology, space and mobility. Work in these fields ranges widely and includes both the analysis of technologies from location-based services in urban environments (de Souza e Silva and Frith, 2010; de Souza e Silva & Sutko, 2009) to new warfare and security practices (Graham, 2010; Bajc, 2010) and histories of sciences of movement such as logistics, which Cowen (2011) explains increasingly organizes commerce, war and security globally. Mobilities studies in particular, positioned at the intersection of geography, communication, sociology and a range of other disciplines is uniquely poised to tackle issues of communication, technology and mobility from perspectives that, traditionally, communication does not.

A key figure in mobilities theory is John Urry, author of *Mobilities* (2007) and co-founder and co-editor of the journal *Mobilities*, first published in 2006. Exploring historical changes in the way mobility is conceptualized, Urry observes that communication and transportation are often studied separately and that the systems that enable the complicated relationship between them are under-explored. Urry outlines a "mobilities paradigm," understanding society as bound by relationships through "discourses of movement" that rely on mobilities (corporeal, object, imaginative, virtual and communicative) and *immobilities*: the technologies, infrastructures, and places that make these relationships possible.

While understanding infrastructure in the context of what it enables is a potentially productive perspective, considering infrastructure as "immobile" and static aligns with the "organismic metaphor" that Manuel DeLanda (2006) argues holds back an analysis of systems in his book *A new philosophy of society: Assemblage theory and social complexity*. Following an assemblage perspective that instead views systems as contingently bound by infrastructure might be one way to think of infrastructures as dynamic rather than static, enabling a *map* and not a *tracing* of infrastructure that would enable *intervention* as opposed to mere representation. More than a history of systems or cultural history of technology, mapping infrastructure would work towards understanding the logics driving the development of infrastructure and the larger systems they support, seeing them as key sites of possibility and potential action rather than set structures.

Stephen Graham (2005; 2009; 2010) is also a central figure in the mobility turn. Graham has done work on infrastructural warfare that has an important place in the present project. His work highlights the importance of thinking about infrastructure in a very material sense, exploring military strategies of targeting "dual-use infrastructure"— infrastructure at the same time civilian and military—in order to de-stabilize control over territory and shake citizen confidence in leadership. In this sense, there is a very real connection between networks and power that the military has only recently begun to explore (beginning around the Gulf War). Graham (2005; 2010) explains that it increasingly appears that this kind of warfare is moving to a network-based cyberattack, which is perhaps the most important implication for my project in that it focuses specifically on the potential for catastrophic cascading infrastructure failure at the hands (or fingertips) of an unknown entity.

Approach

My approach here explores infrastructure as both "smart" and "critical" while grounding an analysis of processes of informationalization in a longer history of infrastructure development, paying close attention to processes of coevolution and the larger contexts in which the process of informationalization plays a key role. In *Aramis: or the Love of Technology* Bruno Latour (1996) explains that "[a] technological project is not *in* a context, it gives itself a context, or sometimes does not give itself one" and argues that it is important to "study the way the project is contextualized or decontextualized" in terms of a network (p. 133, emphasis original). Focusing on the context and network of processes of informationalization for better (smart) or worse (critical), I focus on the ways in which informationalization has produced a context that cuts across a variety of popular, industry, government and military discourses in an effort to understand the logics that support (and sometimes contradict) a desire to make networks smart.

As infrastructures in areas not usually considered under the purview of communication research (i.e. transportation and utilities) are informationalized, the field must consider how processes of integration with information networks expand the potential field of study. This project represents a move toward that goal by focusing specifically on utopian / dystopian discourses of connection, while at the same time understanding infrastructure at the nexus of power formations and as a site of securitization. This approach follows in a long tradition of looking at the logics and discourses that animate communication and technology, including the work of Williams, Carey and Innis. I focus on the informationalization of infrastructure development through a utopian discourse of technological progress (smart infrastructure) that "sells" what appears to be a new

infrastructural ideal and, conversely, a dystopian logic driven by a military security complex that develops a discourse of infrastructure as a site of security (critical infrastructure). Though the main focus of the project is to look at the discursive aspects of this change, I make an effort to acknowledge the material logics of connection and disconnection through practices of connection and disconnection in the electric car, survivalism and infrastructural warfare as well as physical and spatial properties of infrastructure.

This project follows in a tradition of work coming out of a critical interpretative perspective and focuses on the role of knowledge production in organizing infrastructure design and use. Conceptualizing infrastructure in terms of "smart" and "critical" asks us to think about infrastructure from contrasting standpoints that range from discourses that celebrate the economic, environmental and end-user potentials of informationalized and converged infrastructure and those that suggest an increased possibility for cyberwarfare and other forms of attack that leverage increased dependency upon and interconnection amongst infrastructures against national infrastructure as a whole. One way to conceive of the changes wrought by the informationalization of infrastructure is to view this informationalization as a Foucauldian apparatus in order to explore how this process reorganizes infrastructure in new and important ways.

Jeremy Packer's "What is an Archive" (2010) suggests a Foucauldian approach that is particularly relevant to the study of communication technologies as they are implicated in larger organizing logics, or "apparatuses." Presenting a new way of thinking about the archive through a consideration of Giorgio Agambens' *What is an Apparatus?* (2009), Foucault's "What is an Author" and Raymond Williams' *Television* (1974), he suggests seeing the archive as consisting of a range of "discursive and nondiscursive utterances,

statements, and grammars, of architectures, diagrams, and backup plans that work to hold together sometimes-fragile apparatuses" (p. 90). Positioning thinking about the archive among Foucault's evolving conceptualizations of power and increased focus on material as opposed to discursive objects in his later work, he asks, "What is an archive?" (p. 92). Packer outlines the archive as a means by which the apparatus can be understood and explains, "[t]he archive is what results from how one asks questions and where one looks for answers" (p. 100).

Taking *Television* (1974) as an example, he explains that while methods such as textual analysis have a place in Williams' research, an understanding of *mobile privatization* developed instead by viewing "media and communications through a framework that acknowledges their material presence and the attendant force exerted upon lives and landscapes" (p. 94). This understanding, he suggests, calls for a focus on the larger contexts in which media and communication were shaped and made to matter, and demands "a new archive" configured to recognize the apparatus at work (p. 100). Packer outlines five "realms of inquiry" that work toward configuring this archive. He suggests that we first look to "determinators" in the form of "organizations, institutions, or credentialized experts" that have the power to make truth claims about a phenomenon, focusing on discourse that seeks to alter behavior (p. 101). Starting here, we might consider corporations, industry, the government and the military as positioned to make truth claims about the informationalization of infrastructure. A second area of inquiry is to identify "free-floating legitimators" that serve to justify the organization of apparatuses; in the context of the present work, "smart" and "critical" are such legitimators. Third, he suggests that we locate resistance and contestation in order to include in the archive the "full compliment of

competing discourses in their combative play of force," (p. 101) which can be seen in this project in the struggles against the imperative to connect (such as grid-away-from-the-grid living). A fourth area of analysis is "the material functioning of the apparatus" which focuses on the infrastructure of apparatuses, providing "the mechanisms and processes that maintain the necessary movement and flows to keep an apparatus working smoothly" (p. 102), an important if not central element in the present work. Last, the archive must pay attention to subjectification, identifying "cases in which a subject is turned into an object" (p. 102).

I will take as my archive a variety of discourses that demonstrate the pervasiveness of these logics across a number of sites, discourses and practices located in a wide array of historical, government and commercial documents, films, websites, guides, advertisements, news coverage and experiences. As Deleuze notes in *Foucault* (1986), Foucault's archives do not follow a history of what particular authors have said on a topic, but are rather assembled to examine points where power is focused in a particular way "on the basis of the simple function they carry out in a general situation" such as "the rules of internment in an asylum or even a prison; disciplinary rules in the army or at school" (p. 17). The type of power that I am interested in here is the power of informationalization, and I have worked to identify sites at which "informational power" is active. Deleuze argues that:

> One of the basic ideas in *Discipline and Punish* is that modern societies can be defined as 'disciplinarian'; but discipline cannot be identified with any one institution or apparatus precisely because it is a type of power, a technology, that traverses every kind of apparatus or institution, linking them, prolonging them, and making them converge and function in a new way. (p. 25-26)

Along these lines, this project works to understand processes of informationalization, locating it at various sites, in particular moments, and at the center of changing articulations where information is brought to bear in new and important ways. Informationalization cuts

across a variety of institutions, services and daily activities, and affects both the management of the self and of others in important ways. While connections to Deleuze's control society (1997) could be made here, I would rather take the long way around, exploring instead the operation of informationalization in both utopian and dystopian contexts, specifically.

At the core of this project is a desire to re-capture transmission in the study of communication. In *Anti-Oedipus* (1983), Deleuze and Guattari position distribution at the center of production and consumption, indicating a need to focus on the mobility of objects, information and persons. Transmission and distribution are becoming increasingly important, particularly as the ways in which goods are produced and, more recently, the ways that they are consumed have been revolutionized by information technologies. For instance, sweeping changes have occurred in the way media content is consumed over the past several years through the invention of platforms such as YouTube, iTunes, Apple's App Store, Hulu, and Netflix. Such platforms have been made possible by advances in distribution, from shifts to deliver television content digitally via satellite, cable and broadcast as well as massively increased bandwidth that makes sending and receiving large amounts of data in short amounts of time possible. These shifts have made possible on-demand models of viewing where users can manage media consumption outside of fixed locations and timeslots via wireless mobile devices, significantly altering what Williams once described as the flow of television programming (Oswald & Packer, 2011). More than just making analog processes open to digital manipulation through remediation, informationalization is making it possible for users and content providers to accumulate metadata on tastes and preferences, viewing and listening habits, and a range of other habits not directly linked to the consumption at hand, creating new economic opportunities and new opportunities for surveillance.

While materials and energy sources are finite, informationalization has opened areas for economic growth in dynamic pricing frameworks which enable service providers, governments, and users to have more control on the "when, where, and by what means" in addition to the "what and how much." Informationalization makes possible new ways to generate profit in transmission and distribution without producing anything new, even when less is consumed, including dynamic pricing schemes in utilities (varying rates based on supply and demand, selling power back to the grid), transportation (insurance based on location and time of day, road tax based on mileage) and communication (tiered broadband service). These shifts indicate that distribution is a central area in the production-distribution-consumption process from which wealth can be extracted. Before the extraction can happen, there must be a way of collecting data about processes. This is where informationalization comes in, with developments including smart grid, smart transportation, and smart pipe (tiered internet) which are coexistent with the informational mode.

One area where the desire to informationalize is a major point of contention is the ongoing network neutrality debate. While internet traffic was formerly managed along the lines of a "first in first out" protocol that did not discriminate among data packets, advocates of "smart pipe" or "tiered internet" schemes argue that in order to best manage traffic, it is important that the data be prioritized according to type (for instance, time-sensitive activities such as streaming video or performing a remote medical consult will suffer more from jitter and lag than someone downloading a file for later viewing or receiving an email). As technologies have developed that enable packet sniffing – or what equates to peeking inside the data packets as they are being sent in order to guess their contents – internet service providers have worked to demonstrate a need for using these tools to get optimal use of the

network. Packet-sniffing technology essentially adds an information layer to the data, making it possible to manage flows of information in new and different ways. The potential to catch illegal file sharing of audio and video content is of particular interest to internet service providers that are also content providers and have strong ties to media companies (such as Time Warner Cable, formerly owned by Time Warner, and Comcast, which has a majority stake in NBC Universal). Packet-sniffing also has potential for gathering intelligence both at home (domestic surveillance) and abroad (military intelligence).

While adding information layers to processes is not a new phenomenon, digital media have enabled information to be brought into relation with analog processes in new ways and with increased intensity, enabling new practices, services and management techniques. In Carey's classic example of the train, standard time and the telegraph not only enabled the train to be managed more efficiently and safely across space, but had a secondary effect of creating common commodity pricing on a national scale and, by extension, futures markets. While these markets were not the primary motivation for informationalizing the railway, they resulted in important economic developments and constitute an important historical moment at which a discourse of safety was used to propel changes that provided a foundation for an emerging market form. While informationalization today is driven by the desire to make infrastructure smarter and more economically competitive, it is also fundamentally changing the ways that infrastructures are used and experienced, transforming the ways that we interact with the most basic services of contemporary American life. Dystopian discourses of connection are often minimized, with solutions for problems arising interconnection (such as erosion of privacy, cyberwar, cascading failure) framed in terms of increased security (more information layers) rather than boundaries and limits on what should be informationalized.

Chapter Summaries

This dissertation focuses on informationalization, its contexts and environments, and importantly, how it acts as a new form of power that cuts across a range of institutions, practices and technologies. I explore the effects of this new form of power across areas in which utopian discourses of "smart" and dystopian discourses of "critical" infrastructure are present, including the potential for electric mobility to create a greener form of automobility, the dangers of cascading infrastructure failure via networked attack and a smarter approach to war, and finally, a smart survival solution made possible through the creation of a grid away from the grid. Before that, however, this dissertation defines a series of terms that will be used throughout to examine informationalization: terms which are, sadly, in much of the developing body of literature relating to infrastructure, defined differently, used interchangeably with other terms, or not defined at all.

For this reason, in the following chapter I discuss and define key terms relating to this project, including infrastructure, system, network, grid, assemblage and platform. Though some work has already been done in this introduction and elsewhere to define and explain informational society (Castells, 1996) and informationalization as it relates to technologies of screening (Packer & Oswald, 2010), the following chapter takes the term up more broadly as it relates to the specific construction that I am interested in here. "Smart" is also introduced in more detail, representing what Packer describes as a free-floating legitimator, or "particular [term] [which] come[s] to take on such significance that [it] can be used to justify nearly any truth claim across numerous discourses to justify a vast array of initiatives, plans, responses, and resistances" (p. 103). As "critical infrastructure" has a rather long history

rooted in government policy and military doctrine and has already been defined extensively there, its definition and description are a central feature in chapter three.

Chapter two looks at one case where informationalization has been leveraged in support of an emerging electrically powered mobility paradigm. Beginning with a detailed description of the present state of automobility infrastructure, the chapter develops an archive for electrically powered mobility, drawing on early histories of electric cars and a history of the electric streetcar via the trade publication *The Electric Railway Journal*. I briefly examine the recent past of electric automobility via General Motors' EV1, most famously discussed in the documentary *Who Killed the Electric Car* (Deeter & Paine, 2006), and then turn to an analysis of a leading electric mobility solution developed by Better Place. The chapter argues that an emerging discourse of the *smart* works as a free-floating legitimator for an electric automobility paradigm. I aim, as Carey and Quirk suggest in "The mythos of the electronic revolution" (1970/1989), to demystify this sublime through analysis of a handful of interconnected challenges to electric mobility, including mobility on-demand, social and environmental justice, and foreign dependencies.

Following this exploration of the smart sublime via electric automobility in chapter two, chapter three examines dystopian aspects of informationalization in terms of critical infrastructure and key resources (CIKR) as defined and discussed by the United States Federal Government beginning in the 1990s and intensifying in a post-9/11 environment. After discussing the relation between infrastructure and war, I map the changing definition of the term "critical infrastructure" by analyzing an archive of Presidential Decision Directives, Executive Orders, legislative acts, plans, policy documents and reports in relation to national security, safety, the public-private partnership (PPP), and military operations abroad.

Understanding the key role of critical infrastructure and key resources in national security, I then turn to an exploration of infrastructure war as discussed by mobilities scholar Stephen Graham (2005; 2009; 2010) and examine a significant development in infrastructure war: cybermediation. The 2010 targeting of Iranian nuclear facilities with the Stuxnet worm and the ensuing media coverage of the attack will serve as a site for understanding the potential legality of such tactics in carrying out infrastructure war in international conflict now that the existence of *cyberordnance* has been effectively proven. I suggest that while threat of cyber-based attack to achieve cascading infrastructure failure is as yet distant, such threats continue to animate dystopian discourses of connection which, rather than being met with a response that advocates disconnection, work to advance logics of security. Cyber-mediated infrastructure war will also be discussed as a new kind of *smart war* which works on the one hand to reduce allied losses and mitigate immediate loss of life of adversary civilian populations[1], and on the other has potentially serious long-term consequences for civilian populations and target economies.

Having examined imperatives to informationalize and to secure as well as strategies to undo the *net-work* of enemy targets, in the fourth chapter I explore an alternate posture to infrastructure convergence: disconnection. Through an analysis of a variety of "off the grid" discourses, chapter four reflects on what it means to live "off the grid" as well as what it means when "the grid" is off. To interrogate disconnection further, I look to a variety of bunker solutions, including the former government back-up site at the Greenbrier Resort in White Sulphur Springs, WV, and a number of private solutions including shelters built using

[1] While drone attacks (controlled remotely via information networks) have been used to target persons and have resulted in high numbers of civilian casualties, this dissertation makes a distinction between weapons managed via information networks and those weapons which consist entirely of digital code, such as the Stuxnet worm.

abandoned government and military facilities as well as the ground-up solution offered by the Vivos Group. Because the Vivos Solution offers a new perspective on shelter design, I will look to that solution in particular as representative of a contemporary production of spaces of survival, paying particular attention to elements of Lefebvre's spatial triad (conceived, perceived, and lived space) to work toward a knowledge of that space. Elements of the Vivos Group's persuasive messaging will also be explored, particularly the important distinction that the organization makes between survivalism and surviving. Importantly, while survivalism requires a certain degree of disconnecting from "the grid," being a survivor and having co-ownership in a Vivos Shelter is positioned as a survival solution for the *smart subject*. The smart subject position is explored via Foucault's *Technologies of the Self* (2003) and the notion of *askesis* described in Foucault's lectures given on the subject at the Collége de France 1981-1982 (2005).

Through these cases, I work to further understand informationalization as an apparatus that is rearticulating infrastructure according to a new infrastructural ideal and an associated politics of security that are coextensive with both utopian and dystopian discourses of informationalization. First, however, it is necessary to define some key terms that serve to lay a foundation for the work at hand.

Chapter 1: A Series of Terms

In much of the work on contemporary infrastructure, scholars tend to blur the boundaries between infrastructure, systems and networks, and assemblages. This results in work that is not exactly sure of its target. Taken together, these definitional challenges represent a barrier to interdisciplinary collaboration and the development of a meaningful conversation about infrastructure as central to thinking about the way in which we build, maintain, practice, and defend society in the twenty-first century. A distinction between objects of analysis is necessary for moving forward in meaningful ways. This chapter will define key terms in order to provide a foundation for understanding the materials and processes at work in the development of smart infrastructure and the securing of such infrastructure from an array of unknown threats.

Before defining these terms in more detail, I will here provide a summary definition of the major terms. *Infrastructure* consists of the materials and practices necessary in an undertaking, or simply "parts" and "ideas." *Network* is understood here in two senses: first, as a verb—the process of "throwing a net over" or linking parts, and second, and a noun—the result of such a process of linking. A *system* comprises infrastructure and network, and is constituted of materials and practices organized to achieve a certain end. Following this, infrastructure and net-work are brought together to compose what we refer to as systems.

Infrastructure

Issues of infrastructure are often considered important in studies of cities, nations, corporations, and organizations. From highways to sewer lines to 4G wireless services, infrastructure serves as the foundation for a variety of personal, corporate, and government

activities. Research on infrastructure seems mainly to focus on infrastructure use (particularly in urban environments); information infrastructure (II) in corporate, academic, and non-profit environments; and historical analyses of cultural and political aspects of system development and deployment.

One challenge to beginning an analysis of "critical" and "smart" infrastructure lies in the scattered and interdisciplinary nature of the literature. With the term "infrastructure" not coming into use until the 1920s in military contexts as a loan word from French, and in the 1970s referring to public works more broadly, such inconsistency is not surprising (Lewis, 2008, para. 11). Graham and Marvin (2001) argue that infrastructure must be understood from an interdisciplinary or transdisciplinary perspective, though up to that point, work on infrastructure had largely been "inward-looking, technical, and overly-specialist" and failed "to develop critical, cross-cutting perspectives on urban infrastructures and technological networks as a whole" (p. 17).

A recent volume that incorporates many disciplinarily fragmented perspectives on the topic of infrastructure is *Disrupted Cities: When Infrastructures Fail* (Graham, 2009) which claims to be "the first book to peer into the complex processes and politics that surround infrastructure disruptions and failures" (p. xi) and includes work from scholars in fields including geography, environmental studies, political science and sociology. With the topic drawing interest from a wide variety of fields, it is understandable that as yet, authors and scholars have not established common definitions for infrastructure as it relates to other terms such as system, network, and assemblage. In cases where scholars look at a specific issue surrounding infrastructure, most do not take the time to define the word explicitly before discussing the development, deployment, or cultural impacts of technology.

A body of work that directly addresses infrastructure is growing, though as of yet it does not represent a coherent literature organized around a particular understanding of systems, infrastructures, networks, and assemblages. Nevertheless, a few trends seem to hold it together. Much of the work begins with a discussion of what infrastructure is before moving to a discussion of a specific infrastructure, organizational practice, or function relating to infrastructure such as a specific communication infrastructure (see Dourish, 2007), organizational information infrastructure (Star & Ruhleder, 1996, Jansen & Nielsen, 2005) and/or function relating to infrastructure (repair and maintenance, see Graham and Thrift, 2007; co-evolution and convergence, Jansen & Nielsen, 2005). When authors focus on the specific elements necessary to the operation of a system, they are taking "infrastructure"—defined as "a collective term for the subordinate parts of an undertaking; substructure, foundation" (Infrastructure, 2011)—as their object. In other cases, authors gesture toward a secondary definition of infrastructure: "the permanent installations forming a basis for military operations, as airfields, naval bases, training establishments, etc." (Infrastructure, 2011). In a piece on urban infrastructure and U.S. military tactics, Graham (2005) identifies the significance of "dual-use" infrastructures as a centerpiece of U.S. military strategy, a topic that he expands on in subsequent articles and book chapters and as well as in the edited collection *Disrupted Cities: When Infrastructures Fail* (2009) and *Cities Under Siege* (2010).

To complicate an already unclear understanding of infrastructure, there are a variety of special terms that refer to specific "infrastructures" that are used in academia, government, and the media, including: cyber infrastructure; information infrastructure (II), national information infrastructure (NI), and global information infrastructure (GII); critical infrastructure (CI) and key resources (KR); strategic mobility infrastructure; and dual-use

infrastructure. As my focus here is on informationalized infrastructure and security, all of these specific definitions will come into play throughout my analysis. At this point, however, we need a core definition of infrastructure on which to build.

Infrastructure is the material and procedural foundation by which the necessary preconditions for an undertaking are made possible; it consists of both material (copper, rubber, bodies) and discursive (standards, practices) aspects. Importantly, these infrastructures are layered, meaning that in some cases entire systems can constitute the infrastructure for an undertaking (for instance, though National Highways constitute a network, they can also be understood as an infrastructure in U.S. automobility). Because of this, attention to scale is crucial when taking infrastructure as an object of analysis. Methodologically, one must decide which approach to take in following the flow of infrastructure: will the analysis go up (from roads to transportation more broadly), out (all roads in the geographical boundaries of the United States, ones that connect the U.S. to Canada and Mexico, those that exist outside of the U.S. entirely), or down (to the construction of one highway, or the materials that construct it)? What historical frame will the analysis take? In other words, will it focus on present conditions, future trajectories, or historical conditions (and how far back – would the analysis look at roads pre-automobile? Foot paths? The natural flow of rivers as water highways over land…)? Further, such an analysis can be narrowed by topic, from public works or military infrastructures to more narrow analysis of sewers or postal infrastructure (such as the mailbox) or by a criterion around which infrastructure was influenced (speed, bandwidth, reach). Following the paths of infrastructure through time and space necessitates a clear itinerary: where and when will you go and what will you stop for along the way?

This dissertation takes two broad themes as its focus—informationalization and security—and examines the ways that these forces have come to shape the foundations for systems and networks as well as space and mobility in the United States. While limiting the focus to an analysis of the infrastructures and systems in a particular geographic area can be seen as detrimental to a complete analysis of the ways in which informationalization and security play out globally, understanding them in a limited geographical and cultural space will enable a more detailed look at the systems, practices, policies, and reactions to informationalization and security of infrastructure as it serves the needs of the nation, national security, and the citizen/consumer. Given the broad nature of the many kinds and types of infrastructure that could be chosen for analysis, this work is limited by a focus on those infrastructures that have been chosen selectively to illustrate a range of phenomena and processes of informationalization. I will not look at these infrastructures in a level of depth fitting to an analysis of just one infrastructure, as it is logistically impossible in the course of one project to do a complete analysis of all of the infrastructures discussed (from development to composition and analysis of deployment).

That being said, it is important to think of infrastructure as being composed both of material and discursive aspects, and having content and form at all scales. Thinking of infrastructure as simply cables, roads, or wires fails to get at the ways in which infrastructure, particularly at larger scales, is thought, organized, and made to function as part of a larger set. When thinking on the scale of a larger infrastructure set such as critical infrastructure, we must understand infrastructure as also being constituted of various *systems* that serve as the necessary components to broader (and potentially contradictory) economic and national security concerns.

System

While *infrastructure* refers to the material and organizational underpinning for a function, a *system* is that organization of materials and practices articulated to achieve a certain end or ends. This organization can come either from the ways in which the system is designed and actively managed, as is the case with technological systems, can emerge through activity over time as with natural systems, or some combination of the two, such as in social systems. Environmental scientist Donella Meadows explains that "[a] system is a set of things—people, cells, molecules or whatever—interconnected in such a way that they produce their own pattern of behavior over time" (2008, p. 2). While the organization of systems can happen either through intention or environment, "system" focuses on that very organization—the articulation of elements—that produces an outcome. Those elements are infrastructure, and the articulations I will discuss later in terms of net-work and networking.

Unfortunately, many authors taking infrastructure as a focus often use the terms "system" and "infrastructure" interchangeably with little consideration of the consequences. Complications arise when authors use "infrastructure" to refer to what is more commonly known as a *system,* or "A set or assemblage of things connected, associated, or interdependent, so as to form a complex unity; a whole composed of parts in orderly arrangement according to some scheme or plan; rarely applied to a simple or small assemblage of things" (System, 2011). What sets the system apart from an infrastructure is that the system is a complex unity organized to achieve a particular end.

To understand in more detail the muddle created when infrastructure and system are confused, it is helpful to look at a widely cited definition for infrastructure put forward by Susan Leigh Star in her article "An Ethnography of Infrastructure" (1999), in which

infrastructure is defined by outlining nine characteristics: embeddedness; transparency; reach or scope; learned as part of membership; links with conventions of practice; embodiment of standards; built on installed base; becomes visible upon breakdown; is fixed in modular increments, not all at once or globally (pp. 380-382). This definition and its continued use represent a conceptual gray area between "infrastructure" and "system" that must be clarified before an analysis of infrastructure can move forward. In Star's definition, for instance, "the Internet" would not be considered infrastructure. While it is embedded in larger practices, is generally transparent, has an extensive reach, builds on a previously installed base (initially the telephone network), is visible as a larger structure upon breakdown, and exists at a variety of scales linked as part of a larger infrastructure, it is not "learned as part of membership": while many of us consider ourselves internet users, we can hardly be "members" of the internet, and are often rather members of sites, forums, and communities that we access via the internet. But what happens when we read "e-mail" alongside this definition? Interestingly, it more accurately fulfills the requirements of Star's definition, though our more common understanding of email would position it as a practice or system rather than an "infrastructure."

When scholars talk about infrastructure in terms of Star's work, which is so far perhaps the most consistent element of the term "infrastructure" as used in the literature, it becomes clear that her definition, for better or worse, has purchase. Even in the work of Stephen Graham, whose research has in many ways inspired my own, Star's influence is apparent. In *Disrupted Cities: When Infrastructure Fails* (2009), Graham discusses the work of Geoferry Bowker and Susan Leigh Star who suggest that "Good, usable [infrastructure] systems, disappear almost by definition. The easier they are to use the harder they are to see.

As well, most of the time, the bigger they are, the harder they are to see" (p. 7). Here, Graham has taken "systems" and with a dangerous use of brackets, included infrastructure. This slippage is problematic because while people do not *see* infrastructure oftentimes because they simply do not notice it, seeing a large system is impossible! One can be *aware* of a large system, but one can only see its components, or infrastructure. The system is difficult to "see," because rather than seeing with the eyes, it is "seeing" that connotes comprehension that enables the system to be grasped; such seeing requires an understanding of the logics that articulate the system in a particular way at a moment in time in order to achieve a particular end.

As part of Graham's own description of infrastructure, he points to elements such as pipes, ducts, servers, wires, conduits, electronic transmissions, and tunnels which "sustain the flows, connections, and metabolisms that are intrinsic to contemporary cities" and explains that "through their endless technological agency, these systems help transform the natural into the cultural, the social, and the urban" (p. 1). In Graham's definition, we see already (on page one, no less) a conflation between systems and infrastructure. He says that infrastructure sustains flows and connections, and though he explains that infrastructure sustains flows, he moves to a discussion of systems with no further explanation. Why does Graham discuss electronic transmissions, for example, as infrastructure on the one hand and on the other hand explains that infrastructures sustain flows, connections, and metabolisms? He says that systems have technological agency and the ability to transform, but then what is a system? Is a system to be understood as the combination of infrastructure, connections and flows? While I would like to believe this is the case, in this work and other work discussing infrastructure more broadly, there is a conflation between system and infrastructure which at

first may not seem extremely important, but results in a conceptual gray area which can not only hold back the development of an "infrastructure studies" but also have further repercussions in terms of investment, security, and general understanding of technical matters among users. For instance, in issues of funding infrastructure development, sliding definitions of infrastructure and system could mean the difference between money going toward build-out and production of infrastructure elements that would lead to manufacturing and construction jobs and the articulation of elements involved in organizing infrastructure (system development), which would mean money spent on organizational and planning activity at higher levels (with little job generation in manufacturing and construction). To begin to think more critically about the difference between infrastructure and system, I will look briefly to the internet and then automobility as case examples.

To recount a brief history of the internet, remember that it was developed initially as a military technology, and was later utilized in academic research as a communication network. It was designed to connect various hubs of communication in a flexible, redundant network that would withstand nuclear attack. When we think of what "constitutes" the Internet, we could start by thinking about the telephone network as an underlying infrastructure, or more specifically, the line or wireless router from the computer to the modem, the twisted pair of copper wire from the modem to the wall, the wiring in the building that leads to a junction box or utility pole, a large bundle of cables leading to the switching station and the machines and personnel therein, fiber optic backbones designed for long-haul transmission on the phone network, a signal eventually making it to a server in the form of a request from the computer, information being called up and packetized, and the host computer sending it all the way back down the chain to the receiving computer.

This is an extremely basic description: information often bounces around, not taking the most direct route possible, and moves through many more than one or two hubs. Also left out here are the protocols used to packetize information, the hardware and software that compose the computer as a workable machine, the processes through which the information requested came to be digitized and available, the engine which made the information searchable, the browser that made the information browsable, the processes involved in creating secure connections using encryption, certificates, and specialized hardware, and the electrical infrastructure on which information infrastructure relies. All of these components represent “internet infrastructure,” and yet the internet itself is an infrastructure, and the system or application that is most often conflated with it is the World Wide Web (www or simply “web”). Anderson (2010) notes in “The Web is Dead” that: “over the past few years, one of the most important shifts in the digital world has been the move from the wide-open Web to semiclosed platforms that use the Internet for transport but not the browser for display... Producers and consumers agree: The Web is not the culmination of the digital revolution” (para. 3).

To further illustrate the distinction between an infrastructure and a system, consider the automobile. The functioning automobile is a system composed of various parts organized in a particular way to achieve an end (mobility). At a point, removing parts of the car causes to make it cease to be a car. For instance, though broken speakers, a missing back seat, rust damage and broken windows do not prevent the car from being "a car" (though they may represent a change in intensity), once essential components such as steering wheel, tires, and engine are removed, the car is no longer a functional system: the car becomes junk, scrap, car

parts or even, in some cases, a "parts car" (a change in kind). The heap is then no longer a system per se, but an articulation of material infrastructure.

Complicating the infrastructure/system distinction is the variety of scales involved in the analysis of infrastructure. In some cases, Star's definition of infrastructure could be workable, when for instance an entire system constitutes infrastructure for another system. A common example is the system of electrical generation and distribution, which serves as a key component or infrastructure for telephone, television, and traffic systems. Automobility relies on systems of licensing and vehicle registration, traffic lights and signs, highway systems, and systems of fuel delivery and sale among many others.

Importantly, infrastructures have more potential than systems. If I have a wooden board, I can use it as a balance beam, nail it to another board as I build a house, or burn it for heat. If I use it to build a house (a vast organization of materials), burning it to keep myself warm is out of the question, as the board has been incorporated into a more stable organization of materials as a support, or a stud, or framing, losing potential. On the other hand, if I have a set of blocks, I may build a house and play by removing the blocks until the structure collapses. A child playing with blocks implicitly understands the potential of each block to be arranged and rearranged, and does not glue, nail, or fix blocks together: they eventually let castles and houses fall or be destroyed. A dollhouse is a different case entirely. The end result is a house to play in (a structure), not playing with housing (infrastructure).

Infrastructures constitute spaces of movement, force, and power relations. To conceive of infrastructure as a "system" is to discuss it in terms of what current articulations do rather than what their infrastructures enable, and to represent a tracing of the status quo rather than a map that would facilitate understanding of new articulations and bring the logics

guiding those articulations to the surface. What is needed is rather a view that sees infrastructures as spaces affording the direction and re-direction of flows across space and to understand the processes by which these articulations are made. To understand some of the ways that systems are articulated, it is necessary to look to networks.

Network

With the relation between infrastructure and system clarified, the more challenging distinctions between infrastructure and network and system and network remain. Catlaw (2008) has argued that the network has become the root metaphor for our present environment, and as such is a term that is crucial to define before moving forward. In an effort to further distinguish infrastructures and systems, a clear definition of network is necessary. *Network* can be defined in two main ways: first, as a practice of making links (see Wiley, Moreno & Sutko, 2011 and Wiley, Sutko & Moreno 2010)—to literally do the work of linking or "net-work"—and second as the manifestation of such linking practices. Throughout my work, I rely on networking in the first sense, as the work of connecting, linking, and articulation; network in the second sense (the manifestation of such practice) is in most cases best described as either an infrastructure or a system.

One way in which networks have been examined is in the context of social ties. As individuals are increasingly members of both local and global groups (such as being a member of a university community as well as a world-wide *Stargate SG-1* fan community) the ways that they maintain extended social networks, activate social ties through face-to-face meetings, and navigate global flows determines the extent to which they can affect their social space. Now that it has become possible for citizens to reach out across the globe not

only for media access, but for personal and business communication, we should understand which individuals have these levels of access, how they use communication and transportation technologies in their daily life, and the ways in which they use these technologies to produce and alter their social space. Looking specifically at networks as relational, scholars such as Barry Wellman, John Urry and Juan Carrasco have focused on the ways in which individuals create and maintain social networks. While Wellmans' Connected Lives project (2005) is designed to achieve a deeper understanding of the role of information technology in the home and in social networks, others such as John Urry have examined the role of travel and face-to-face meetings in the maintenance of social networks.

In *Connected Lives: the project*, Wellman and his colleagues (2005) discuss the transformation of networked groups from small stable neighborhood and village groups to globalized place-to-place networks facilitated by increased transportation and communication technologies. Citing a shift from place-to-place networks, Wellman and his colleagues argue that the present person-to-person model of networks is contingent on the individual's ability and motivation to establish and foster connections that will create opportunities. Carrasco and colleagues have also participated in the Connected Lives project, looking to the ways in which ties are maintained across space, finding agency in these networks as tied to the population of connections rather than the attributes and ability to activate those ties, arguing that power rests in the sheer number of connections. The Connected Lives study seeks to further understand the operation of these networks and the phenomena of *networked individualism* (see Castells 2000), with the goal of further exploring the role that Internet communication technologies (ICTs) play in social interaction.

In contrast with research on the nature of social networks, John Urry's work has focused largely on travel and mobility. Discussing the "six degrees of separation" hypothesis at the center of much social network analysis in the social sciences, Urry (2003) argues that limitations to analysis include a neglect for the degree of "meetingness," or occasions that create, activate, and reactivate social networks, and a focus on the nodes in networks that leads to a neglect for the very things that connect nodes, from events to infrastructure. Urry suggests that networks only function if they are "activated" through "occasional co-presence" that requires travel, which means that the generation and maintenance of networks is not free of expense, and further that analyses focusing on nodes rather than links does not address the connection between social ties and the material worlds that underpin them (2004, p.17). The complex nature of the relationship, he argues, must be understood through not only forms of mobility, but also the immobilities that make them possible, including technologies, infrastructures, and places, focusing on a need for attention to the practices and infrastructures that make social networks possible. Rather than focusing on the result of networking practices (social networks) this asks us to look to the practice of creating and maintaining these ties, or the net-work itself.

In addition to work that focuses on communication between individuals and social networks more largely, much has been gained from an analysis of network forms—a focus on the shapes of networks that result from various communication practices and infrastructures. In their study of digital and biological networks in *The Exploit* (2007), Galloway and Thacker examine the nature of networks and the ways in which weaknesses in them can be exploited by viruses (both digital and biological). Galloway and Thacker argue that power in networks "is based on a dialectic between two opposing tendencies: one

radically distributes control into autonomous locales; the other focuses control into rigidly defined hierarchies" and argue that at present, "All political regimes today stand in some relation to networks" (p. 19). Further, Galloway and Thacker argue that as "the horizon of control," networks should be examined through a process of individuation that considers both the general (types) and the specific (a specific network). An analysis of both logics that seem to be organizing infrastructure as well as the systems that make up larger constructs such as "smart" and "critical" infrastructure will help me work through these concepts.

Understanding networks as a horizon of control is not new, and in fact has been a focus in military doctrine over the past several decades in work that has the attention of the United States Military, such as Arquilla & Ronfeld's *Netwar* (1996), which classifies, explains, and elaborates network forms and identifies new challenges in warfare and security. The focus has not been on security alone, however; the work has also highlighted the ends to which the United States is willing to go to maintain security through having a good offense. Such analysis of the criticality of networks has led to developments in military doctrine that have resulted in redirecting attention from the front lines to communication infrastructures, roads, and power lines themselves in an effort to disrupt and undo the network of enemy targets. Often, such strategies target critical infrastructure sites and key facilities. In *Control and Freedom* (2006), Chun points out that the U.S. carried out bombing campaigns in Iraq in the late 1990s to dismantle a developing fiber optic infrastructure, working to secure network superiority by undoing the net-work of another state. Grahams' work on infrastructural warfare (2009) presents a detailed analysis of network-targeting strategies in this material sense, particularly the targeting of "dual-use infrastructure" in U.S. and Israeli military operations abroad such as power and water infrastructures in order to further de-stabilize

power of enemy regimes. There is a very real connection between network and power that the military has only recently begun to explore (beginning around the Gulf War). Increasingly, this developing doctrine is moving to a cyberattack approach. Arquilla and Ronfeldt wrote in 1996 that "it takes networks to fight networks," and military officials seem to be focusing on finding ways to match their strategies with those of terror networks which are asymmetrical (rather than applying force to force, apply force to a target such as the World Trade Center or critical infrastructure and key resources more broadly) (1996, p. 82).

Grid

In defining infrastructure and system, we must also look to another much-used term: "the grid." How does this construction function to define either an infrastructure or a system? What does it refer to? Is it an infrastructure, system, or network form? While a content analysis of news and trade industry media would most clearly indicate the nature of word use, I will here look to a few case examples in order to develop a workable definition of "the grid" that will be examined in more detail in chapter four, when I look at survival solutions.

"The grid" generally refers to electric, transportation, and information networks and at other times to infrastructure in general as in *On the Grid* (2010), *Off the Grid* (2010), and *Off the Grid: Life on the Mesa* (2007). The very notion of a grid brings to mind an organized network designed for the transmission and distribution of flows, be they material, electrical, or informational. As a network form, a grid is only as such so long as it is active and can function to capture flows (as in a search grid) even if it fails to capture all flows (going "off the grid"). There are times when grids completely fail to function, often because the flows managed by a given grid overwhelm the network design (gridlock) or cause cascading failure

(fire sale). While one of the most discussed cases of grid failure is the 2003 blackout in the Northeast United States, everyday instances of local power outage and gridlock illustrate the same point: while grids move energy and people, they can fail when disrupted or overloaded, making the protection of material infrastructure and the management of flows on the network of critical importance. "The grid," then, is one way of articulating infrastructure: one of many potential network designs for a system. Again, the main characteristic that distinguishes the grid from other network forms is its use in managing flows—of information, people, energy, or substances—from sources to sites through transmission and distribution or collection. Despite their apparent fixity, grids can be altered, and they serve as a key site for processes of informationalization that promise to make them better, faster, and stronger.

Assemblage

One way to think about solving these issues is by thinking of infrastructure in terms of assemblage, focusing on the ways in which infrastructure is articulated into assemblages rather than used to construct systems. I am not merely calling for a change in analytic, but rather suggesting that unlike the ways in which large technological systems were conceived of in the past as static and enduring, today's systems are rather conceived of as distinct from the infrastructures that support them. Such a distinction is clear in the idea of the "constant beta" in software development, in which the software or service is more or less complete, but is continually undergoing development: the essential function of the system remains intact, though new features will become available and old bugs will be fixed. The servers that your email is stored on will change, the code will slowly change, and the ways in which you are able to access your email will also change. All this being constant, the essential service that

your email provider provides will remain stable. The system is no longer inherently tied to its infrastructure – rather, infrastructure is articulated and re-articulated in order to best serve the changing needs of the system.

Understanding that "the grid" refers to a general way of organizing infrastructure to facilitate systems of transmission and distribution, we know better than to assume that any particular piece of infrastructure "makes" the grid. In fact, think of the many power plants that have been built and decommissioned, the miles of electric transmission and distribution lines and utility poles that have been added or replaced, and the incorporation of new software and hardware for managing load and obtaining outage and use information. While many components of our electrical infrastructure have been in use long beyond their expected service life, notions of the electrical grid as a static system prove false when thinking about the ways in which electrical service has been managed as a system that is open, evolving, and made of changing parts and processes.

A key advantage of thinking through systems as assemblages which are contingently bound rather than as organismic wholes is how it enables a focus on process. Such an understanding is productive when thinking about changing articulations of infrastructure which can be understood as an articulation of technics (materials) and techniques (logics) in a given territory over time. In explaining the way that assemblages form, Deleuze and Guattari ask us to begin by thinking of an undefined space upon which logics establish relations between elements to produce a temporary whole (1987, p. 70). This temporary whole, or *assemblage*, consists of the sum of parts and relations between elements. Deleuze and Guattari argue that classifying assemblages and the logics they execute is "The most important problem of all," and suggest that classifying assemblages is a three-step process

that entails: 1) identifying the territoriality that the assemblage envelops; 2) distinguishing content from expression; and 3) identifying lines of deterritorialization that open up onto other assemblages, spaces, and machines (p. 71). Seeing infrastructure as assemblage means that we must look first to the territory held by infrastructure through the management of flows. The moment that this infrastructure breaks down, the relations and spaces are deterritorialized and opened to reterritorialization: the texture changes. Distinguishing content from expression – or the material from the organizational—is the second task. The third task is perhaps the one that I am most interested in here: understanding how infrastructure – particularly informationalized infrastructure – opens up onto other assemblages such as those of economy and national security.

In *A new philosophy of society: Assemblage theory and social complexity* (2006), Manuel DeLanda quotes Deleuze's *Empiricism and Subjectivity* to discuss the emergence of the pragmatic subject, citing the following passage as a place where Deleuze talks about the difference between systems and assemblages that demonstrates that an assemblage becomes a system when organized to achieve particular ends:

> The subject is the entity which, under the influence of the principle of utility, pursues a goal or an intention; it organizes means in view of an end and, under the influence of the principles of association, establishes relations among ideas. Thus, the collection becomes a system. The collection of perceptions, when organized and bound, becomes a system. (Deleuze, quoted in DeLanda p. 49)

So why would an assemblage perspective be more useful than a system or network perspective when considering infrastructure? DeLanda argues that an assemblage perspective is desirable for looking at the nature of relations between elements: in contrast to thinking through the "organismic metaphor" that sees systems as totalities that rely on *relations of interiority* which are *logically necessary*, an assemblage view sees wholes as "characterized

by *relations of exteriority*" in which parts are interchangeable and can exist independent of connections which are only *contingently obligatory* (p. 9-10). This demonstrates a potential fluidity in the way in which infrastructures are articulated, and is useful in that it can lead to a productive understanding of the development of communication, transportation, and utilities networks as contingent and coevolving rather than whole and static. Thinking in terms of assemblages as contingently bound elements rather than as static entities is not only a more accurate way to understand the relations between elements in a system, but can help us to expose points of intervention and resistance. Further, when thinking in terms of infrastructure, such a perspective forces one to think about material infrastructure, system ends or objectives, and the organizational logics for achieving those ends, in turn, as contingently bound rather than static and therefore more flexible and open to rebuilding, repurposing, and reconfiguration.

Positioning infrastructure, network, and system alongside terms from Deleuze and Guattari's discussion of assemblages, Figure 1 takes the car-driver relation as an example to demonstrate the ways in which these terms can redescribe large-scale phenomena. Of course, when thinking about automobility more broadly, a number of other relations could be diagrammed, including petroleum products, highway infrastructure, specific components in the engine, etc. While a systems view in the organismic fashion might say "the vehicle, made of metal and plastics and fueled by gasoline is driven by a driver in the system of automobility," an assemblage perspective looks at the play of elements in an auto-mobile assemblage. Understanding that these elements are loosely articulated and not fundamental, we might ask from an assemblage view, "must the substance of the form be metal or have a gasoline engine?" and even, "must a human do the driving?" Thinking through systems

instead as assemblages encourages examination of relations as presently configured, in the middle of the process, rather than as the inevitable and inflexible products of history.

Terms in Relation to the System of Automobility / Auto-mobile Assemblage

		Form	Substance
Infrastructure	Content	Vehicle	Metal, Plastics, Gasoline
Network	Expression	Driving	Driver
System	Assemblage	Automobility	

Figure 1: The system of automobility and the auto-mobile assemblage.

While assemblage conceptualizations do not necessarily contradict other mainstream definitions of systems, such a perspective enables systems to be seen as more contingently bound than the "organismic metaphor" suggests. While systems theory might have traded the machine metaphor for an organismic one to describe the processes of systems, an assemblage view enables us to see that connections in systems are far more contingent than necessary. Let's take "television" as an example: "programming" is only contingently bound to analog or digital terrestrial broadcasting, cable, satellite, DVD release, as well as a host of internet video platforms (Hulu, iTunes, Netflix). Any one of these delivery systems de-linking from television doesn't necessarily "kill" television, as we saw with the end of analog over the air broadcasting in 2009. Thinking in terms of assemblages helps up to see such distinctions, particularly when taking multiple scales into consideration as systems are re-organized to serve as infrastructures for the purposes of national security (as critical infrastructures) as well as convenience and commerce (as smart).

Platform

One way to talk about the ways in which infrastructures are contingently bound rather than holistic is to look to areas where the most growth is occurring today – in platforms. *Platform* can refer to a raised area, as in a railway or oil platform, a launch point, or a framework for development as in computing and automobile design. In this work, platform refers to a specific articulation of existing infrastructure, devices, and software designed to facilitate further development and deployment of products, services, and infrastructure. Platforms differ from systems in that while they consist of infrastructure arranged to achieve an end, that end is not specific. Further, platforms are not closed or static, but are rather re-arranged on a continual basis. Graham and Marvin explain that the shift from the modern infrastructural ideal to splintering urbanism was facilitated by factors such as neoliberalism, changing regulatory regimes and informationalization (2001). These same forces have created a market for platforms and off-the-shelf solutions that increasingly present commonalities across systems, which enable new economies of scale, but also increased threat vulnerabilities.

For instance, many communication scholars have begun to examine social media platforms such as Twitter and Facebook in terms of social capital, their use in developing relationships between organization and their publics, and organizing social movements (Ellison, Steinfield & Lampe, 2007; Eyrich, Padman & Sweetser, 2008; Bratich, 2011). Because users do not have to create individual web pages that require design and technical skill, or perform in-depth research to locate ties, these platforms represent a low barrier to entry for organizations, communities, and individuals. At the same time, these low barriers to entry present increased concern about privacy, spamming, and hacking: if vulnerability in

Facebook's software opens one organization's page to hacking, it opens all such pages to hacking. The economy of scale works in both directions.

While the hacking of a Facebook or World of Warcraft account has consequences for a users' digital identity, the use of off-the-shelf solutions in critical processes presents the potential for material disruption. This dissertation explores platforms through an analysis of Better Place's electric automobility charging solution, discussing the role of Siemens control units in the attack on Iran's nuclear facility at Nantz, and the Vivos shelter solution as a platform for survival. Understanding these articulations of infrastructure as platforms rather than systems shifts the conversation from one about the development and deployment of systems and their use to one centered on the ways in which these articulations have been thought in terms of connection, disconnection, reconnection, and potential for reconfiguration. These complex articulations are made possible through informationalization.

Informationalization

In *The Rise of the Network Society* (2000), Manuel Castells makes a point to clarify the many claims that we are now living through an age often referred to as "Information Society." Explaining that information has been central throughout the ages, he explains that we should rather think of the current context in terms of an "informational society" in which informational denotes "a specific form of social organization in which information generation, processing, and transmission are transformed into the fundamental sources of productivity and power, due to the new technological conditions that arise during this historic period" (p. 21). Semantically, this distinction reflects an equivalence between industrial society (industry-driven rather than "industry society") and the present information-driven

society (in the use of "informational" rather than "information"). Castells argues that the base structure of informational society is networked, and that many of the features of informational society are driven by this networked base.

Castells also uses the word "informatization" in his footnote on informational societies (2000, p. 21). Informatization and informationalization both refer to processes by which information comes to be integrated into processes, practices, and other functions. Chow-White writes of informationalization that "[t]echnologies and the classification systems that utilize them tend to make invisible the myriad of decisions that create them… the seemingly descriptive representations derived from information infrastructures in fact naturalize a whole set of practices, procedures, and ideological premise" (2008, p. 1173). In this dissertation, I examine the ways in which such processes of informationalization represent and enable new practices and processes, but also examine the ideological premises on which they rely and are constructed. Specifically, I look at the possibilities and promises of informationalization of infrastructure as well as the ways in which information is leveraged in the development of smart systems.

The processes of digitization and translation add new streams of data as well as new avenues of control. While networks such as the telephone and electric grids pre-date the digital, they are in a sense being made digital (or compatible with the digital) through informationalization. Informating adds a data layer, and enables new possibilities in the transmission and distribution of energy, information, goods, and persons as well as vulnerabilities in personal, national, and economic security. Informationalization at the level of infrastructure represents opportunities for a splintering urbanism, but more than that, the manifestation of what Deleuze and Guattari claimed in *Anti-Oedipus* – that "society is

schizophrenizing at the level of its infrastructure, its mode of production, its most precise capitalist economic circuits" (1983, p. 361). It is this "schizophenization" that this dissertation examines through the lens of informationalization, looking to the ways in which conflicting drives to open and secure infrastructures creates a kind of madness managed through economic, military, and governmental logics.

Smart

While Catlaw (2008) argues that the network serves as the root metaphor for our society, the late 2000s saw the development of new ways of talking about how information technology was changing the many networks we rely on. With the understanding that many pre-internet systems in transportation, utility, and communication are already networked or connected in some way, a new metaphor for thinking about the articulation of information networks with the infrastructure of daily life was needed. One could not simply refer to the electric grid as "networked"— of course it is networked—it *is* a network. Instead, as information systems converged with pre-digital technologies, a new way of talking about this informationalization was needed, and industry seems to have settled on "smart."

Smart has been leveraged to describe a new articulation of infrastructure, information technology, and devices across infrastructure development projects, policy, and culture. IBM's "Smarter Planet" campaign claims that we have moved into a smart decade and positions the company as a leader across multiple markets from city planning and education to infrastructure and transportation. IBM's campaign—large, well-funded, and multi-sector—situates informationalization (more simply, "smart") at the core of progress. While General Electric's "Ecomagination" campaign does not explicitly leverage "smart" as a

metaphor, its combination of ecology and imagination often involve smart solutions, from new articulations of electric and information infrastructure to fuel a changing automobility system or high-technology wind and solar projects.

Tied with notions of convenience, progress, and "green," *smart* can be seen as a central component in a new technological sublime that includes smart grids, smart metering, and smart phones and represents a shift in the ways that information is leveraged in communication, transportation, living, and energy distribution. The term often stands in for a variety of other ideas about what consumers want from technology, including personalization, interoperability, convenience, and environmental sustainability. This dissertation explores "smart" in three contexts—automobility, war, and survival—in order to further understand the smart sublime, smart war, and the smart subject. Through this examination, I hope to demonstrate how such rearticulation demands attention at the level of infrastructure in order to demythologize the "smart sublime."

The notion of smart and a developing "smart sublime" works to open up new potentials and opportunities for modulating capital though connectivity and focuses on new markets in transmission in addition to production and consumption. I will begin by looking to infrastructure as smart through electric mobility in the U.S., beginning with an early history of electric mobility and continuing to the present with an analysis of a rebirth of electric automobility, which in essence depends on at least four major areas: the standard automobility system (which itself comprises a variety of other infrastructures including road and highway networks, petrochemicals, manufacturing and more), electric transmission and distribution, charging infrastructure, and communication networks.

A New Infrastructural Ideal

Having defined the key terms, the next three chapters explore the informationalization of infrastructure. First, I examine the automobility system and Better Place's platform for electrically powered automobility as resonant with the *smart sublime*, paying particular attention to the role of informationalization in enabling a shift away from petroleum-based mobility. Next, I look to the development of the term *critical infrastructure* and the present development of cyber ordnance as a weapon that not only targets information networks, but also uses cyber infrastructure as a vector for targeting legacy infrastructures made smart through informationalization in an intensification of *smart war*. In the last chapter, I focus more specifically on the grid in terms of a network form that serves as a metaphor for the necessities of modern life. I show through an analysis of survival solutions that the grid has come to serve as a framework for post-grid living through platforms that present "a grid away from the grid" as a model for the survival of the *smart subject*. Through these analyses, I demonstrate the emergence of a new infrastructural ideal and associated politics of security that are coextensive with both utopian and dystopian discourses of informationalization.

Chapter 2: Electric Automobility and the Smart Sublime

Automobiles are a driving force in the U.S. economy. The Economic Census reflects that in 2007, sales for motor vehicle and parts dealers exceeded $890 billion, more than was made at grocery stores, clothing stores, and furniture and home furnishing stores combined (U.S. Census Bureau, 2009). Automobiles represent not only a significant economic force but also a cultural force and are tied to notions of prosperity, freedom, and social mobility. Serving as an environment in which communication technologies are tested, miniaturized, and networked, the automobile also constitutes a key site of informationalization and point of infrastructure convergence. From the incorporation of gauges that indicate the amount of fuel available in early automobiles to multi-function internet-ready voice activated displays in the automobiles of today, the car represents both a technology designed to screen the environment for the driver and a site for screening technologies (Packer and Oswald, 2010).

Automobility also represents a key space in which Americans consume petroleum products. As concerns about instability in the Middle East combine with predictions that we are already post-peak oil (the argument that half of the available oil from reserves around the world has already been extracted), environmental concerns take a back seat to issues of national and economic security in reinventing automobility. Though moves to ensure a clean energy future in the U.S. have focused on the development of renewable power sources such as solar and wind power, with “clean coal” and natural gas comprising the fossil-fuel elements of clean energy, our cars do not run on sunshine; they run on gasoline. This could change, but it would require the cooperation of government, utilities, manufacturers, investors, and, importantly, drivers.

In the 2011 State of the Union Address, which focused on innovation, education, and infrastructure, President Obama called for the United States to be the first country with a million electric vehicles on the road, a goal that he set for 2015. While electric cars are clearly an innovative solution, they are not the only way out of the petroleum-based automobility system that has reigned for more than 100 years around the world. Hydrogen, biofuel, and solar-powered vehicles have all been proposed as alternatives to the present gasoline-fueled automobility system, accompanied by calls for more development in public transportation, walkable communities, and non-motored transportation. Why this emphasis on the electric car? One reason may be that the promise of the electric car can be summarized in a word: smart. Electric cars are networked, digital, and personal – three features which begin to explain why the electric car will succeed where the hydrogen highway hit roadblocks.

In this chapter, I look specifically at the electric car as the archetype for the smart solution, focusing first on the vast infrastructures of the system of automobility (Urry, 2007) and history of the electric car, its origins in the trolley system, and discussions of the "lock in" of a petroleum-based automobility system in the United States for the better part of the 20th century. I then look to the Better Place electric vehicle solution as an example of current efforts to revive the electric car, specifically the way in which they frame their solution to the challenges presented by electric automobility as being a matter of smart infrastructure deployment. In the concluding part of the chapter, I address a range of issues tied to electrically powered automobility, the on-demand nature of the present mobility system, environmental justice, and issues of foreign dependencies. First, however, it is necessary to discuss one of the main contexts produced by informationalization: the smart sublime.

The Smart Sublime

In *The Machine in the Garden: Technology and the Pastoral Ideal in America*, Leo Marx looks at a history of technology and pastoralism in America, including the move away from the United States as a purely agricultural economy to an industrial one. Marx notes that fascination with and awe of the mechanical led to writing that praised developments and technologies, writing that he terms "the rhetoric of the technological sublime." He cites an example of an article where the editor of the *Cincinnati Inquirer* indicated that animals and people alike were in amazement and fear of the power of the locomotive (2000, p. 195). Marx explains that this way of communicating about technological progress was adapted by early American writers such as Ralph Waldo Emerson and Herman Melville (2000).

In "The mythos of the electronic revolution" (1970/1989), James Carey and John Quirk argue that Marx's identification of the "rhetoric of the technological sublime" can be seen in a new construction: the rhetoric of the *electrical sublime*. Carey and Quirk chastise the scholarship that celebrates the electronic revolution, explaining that this celebration "is a process whereby the world of scholarship contributes to the cults of engineering, mobility, and fashion at the expense of roots, tradition, and political organization" (p. 138). Their call is one to "demythologize" the relation between "technics and myth" (p. 140).

In a later article titled "Historical pragmatism and the internet" (2005), Carey explains that "The literature of the electrical sublime crested in the 1990s when traditional hopes were tied to the internet" and the infrastructures that made them possible (p. 445). He argues that September 11, 2001 signified the end of the 20th century in the United States– "the 'great awakening' from the slumber of the previous decade" in which the literature about the internet was representative of the electrical sublime and was largely "politically

and morally irresponsible" (p. 445). He argued that this research was flawed in three regards: it was not historical enough; it did not look at coevolution of the internet with other technologies; and it failed to examine the larger cultural, political, economic, and religious contexts of the internet. He suggests that rather than thinking only of the borders being erased in all of these changes, we should instead examine the new borders that are constructed.

Slack and Wise (2005) explain that while Marx's description of the technological sublime was a mechanical one that mainly focused on industrial machines and Carey and Quirk focused on the electrical sublime, we may have moved to a new form of the technological sublime entirely, the *digital sublime* (p. 18). Though this digital sublime is not elaborated in more detail, Slack and Wise introduce the concept in order to discuss the ways in which the "progress story" of technology has been leveraged to convince people to live in particular ways, to sell products, and to control and judge others. While the digital sublime is surely one that demands further exploration (particularly as the digital is used to serve as proof of progress without thorough examination, as is the case with the U.S. digital television transition), here I am interested in looking at the *smart* sublime. Do processes of informationalization truly represent that promise of progress that they inspire? Is "smart" really *smart*?

A second concern here is the way in which "smart" acts as what Jeremy Packer (2010) describes as a *free-floating legitimator* (terms which justify the organization of apparatuses) for the informationalization of infrastructure. While Packer has identified safety as one such legitimating factor for a variety of programs and projects that have worked to govern the mobile conduct of subjects (including the incorporation of communication technologies into mobile spaces, as with the CB radio in the automobile), I am interested here

in the ways in which smart technologies have been leveraged in efforts to informationalize transportation infrastructures. To that end, I will begin by discussing the current state of both the material infrastructures and the functioning of the system of automobility before examining the history of electric mobility specifically in terms of what Urry (2007) describes as *series* and *nexus* systems. I will then discuss the efforts of the California Air Resources Board to make zero emissions vehicles (ZEVs) available to consumers, as was documented in *Who Killed the Electric Car?* (2006), and then move to discuss how the resurgence of the electric car in the early 2010s is being driven by a discourse of "smart." Finally, I examine the electric car as part of the smart sublime by pointing to a number of challenges raised in counter discourses to "smart" as well as promises of a smarter grid and a smarter car.

Infrastructures of Automobility

While the marvels of modern communication technologies were once imagined to eventually thin the morning traffic of daily commutes, a steady rise in the number of vehicles on the road has resulted in continued wear and tear on Americas' highways, byways, toll ways, tunnels and bridges. In Raleigh, North Carolina, where the population has more than doubled from approximately 150,000 in 1980 to estimates upwards of 400,000 in July 2009 (Hoyle, 2010), the widening, resurfacing, and redesigning of highways, roads and streets is commonplace. Raleigh is far from the only place where the road work is never done: drivers of I-95, the nation's longest north-south interstate, are also familiar with the joys of never-ending construction, maintenance, repair, widening, and improvement (most recently in the HOV lanes south of Washington D.C.).

In America, automobility is still a central component, if not the keystone, of mobility. With a 2008 population of approximately 304 million, the U.S. was home to nearly 256 million registered vehicles, more than half of these (137 million) passenger cars (Research and Innovative Technology Administration, 2010). The U.S. Department of Transportation Federal Highway Administration estimated that in 2008, more than 87 percent of the U.S. driving age population (16 and up) had a license, and drove nearly three trillion vehicle miles of travel on more than four million miles of interstates, freeways, expressways, arterials, collectors, and local roads (2011).

In 2009, the Consumer Assistance to Recycle and Save Act (CARS Act, 2009) and a later appropriations bill pumped a total of 3 billion dollars into the automotive industry (National Highway Traffic Safety Administration, 2009). In addition to a $39.7 billion budget in 2009, the American Recovery and Reinvestment Act supplied an additional sum of $27.5 billion stimulus dollars to America's roads and bridges for a total of $67.2 billion. The enacted budget for 2010 estimates more than $41 billion for the Federal Highway Program, with a slightly higher request in 2011 of more than $42 billion. Of the total U.S. Department of Transportation [USDOT] budgetary request of $79 billion, money marked for roads and bridges through the Federal-Aid Highway Program constitutes more than half of all requested monies, with this one program amounting to more than the operating budgets of the Federal Aviation Administration ($16.4 billion), Federal Transit Administration (more than $10 billion), National Highway Traffic Safety Administration ($878 million) and all other transportation funding areas—including shipyards, locks, pipelines, and rail—combined (USDOT, 2010).

This figure merely represents the program distributing funds at a federal level. Statistics for total highway spending for 2007 compiled in a 2008 Federal Highway Administration report note that while federal moneys towards highways from the Federal-Aid Highway Program totaled approximately $33.5 billion, this represented a mere 16.6 percent of the total highway spending combining state and local, toll, and other moneys at more than $201 billion; and that's just *highways* (Federal Highway Administration, Highway Statistics 2008, Table HF-1). In addition to more than four million miles of highways and roads and the money to build and maintain them, millions of drivers driving more than three trillion miles every year in their more than 250 million vehicles, are fueled by approximately 8,989,000 barrels of motor gasoline — or 378 million gallons— per day (U.S. Energy Information Administration [EIA], 2011a). The U.S. imports about 9.8 million barrels of crude oil and roughly 3 million barrels of other petroleum products (such as gasoline) daily (EIA, 2011b). While the U.S. produces more than 5 million barrels of oil (a total petroleum product production of 7.2 million barrels) per day, a total consumption of 18.7 million barrels daily ranks the U.S. as the number one global consumer of oil at over 20 percent of daily global consumption, while ranking third in top world oil producing countries at more than 8,500 barrels of oil per day in 2009 (EIA2011b). According to the EIA, 72 percent of our total oil consumption in the U.S. is used for transportation.

The System of Automobility

In looking at the various ways in which systems of circulation and repetition have enabled man to master the natural world, John Urry identifies four features of the "mobility systems" of the 21st century: they are increasingly complicated, interdependent, dependent

on computers and software, and vulnerable to "normal accidents" (p. 14). As technologies such as public transit and street lighting discussed by Raymond Williams in *Television* (1974/2003) contributed to a "public mobilization" of private life, technical operations were concealed from the end user, as public and distributed use was exercised with centralized expert control. Riders became mere objects in the railway system, Urry writes, which "involves propelling passengers through space as though they are parcels. The human body becomes like an anonymized parcel of flesh, 'shunted' from place to place, just like the other goods that get moved around the system" (Urry, p. 94 discussing Thrift 1996).

In taking *systems* of circulation as his focus, Urry makes an important distinction between *series* and *nexus* systems, which will serve in this chapter as crucial concepts for understanding the present automobility system and the evolving electric car infrastructure. Series systems, he explains, are those systems where parts function independently (the automobile) while nexus systems require many different parts working in concert for a system to be effective (the train). While the system of automobility is highly dependent on the production of vehicles, construction and maintenance of roads, training of drivers, procurement of fuel and so on, series and nexus systems are best understood as two ends of a continuum where the focus is on the level of synchrony required: while automobility can be relatively asynchronous with drivers fueling up, travelling, and stopping at their convenience, rail transportation requires high levels of synchrony, with trains departing, stopping, and arriving on time tables in order not only to be useful for passengers in terms of scheduling, but also to avoid oncoming trains. While series systems require storage capacity and the adoption of protocols, nexus systems require fixed networks and *informationalization.*

Railways have long been discussed in terms of the larger cultural transformations that accompanied their rise: a national identity, new organizational management techniques, the idea of a landscape, and a right-of-way network that has facilitated the deployment of infrastructure from the telegraph to fiber optic cables (Carey, 1989; Bradley, 2004; Schivelbusch, 1977/1986; Hecht, 1999). In *Mobilities* (2007), Urry focuses on the impact of railways on the experience of time and space, arguing that these were the first mobile nexus systems. What is perhaps the most significant socio-technical advance concerning the railway was the development of standard time facilitated by the telegraph: "The telegraph could send time faster than a railroad car could move; and therefore it facilitated the temporal coordination and integration of the entire system" (Carey, 1989 p. 174). The timetable, at its most basic level, *informationalizes* the train: speed and movement could be anticipated, making departure and arrival predictable and reducing the chances of collision. With an added information layer, rail travel /transport became more efficient, leading to further expansion of nexus systems.

Informationalization, then, is a practice which adds information in order to make a process more efficient. In the 20th and early 21st century, the U.S. continued to informationalize national space, persons, and resources through programs including the assignment of codes under the Zone Improvement Plan (ZIP) which enabled the more efficient delivery of mail, the issuance of passports (and their reboot under the REAL ID Act of 2005), and ongoing efforts to informationalize the airwaves. Beginning with radio and extending later to television and other wireless communication, management of the airwaves required information layers that would enable spectrum allocation, demarcation of broadcast footprints, scheduling, and eventually clear channels.

Williams situates broadcasting as part of a shift to an emerging mass culture, accompanied by a boom in consumer durables such as home appliances and automobiles, contrasting this "new kind of technology for which no satisfactory name has yet been found"—a form of *mobile privatization*—with public technologies (nexus systems) of the early 20th century (1974/2003 p. 19). Williams' observations of these technologies and his construction of *mobile privatization* to characterize them reflects the tendency of these technologies—that we might understand as series technologies—to add freedom of movement not possible in a previous era dominated by expert-controlled nexus systems. On a track closely parallel to Williams, Urry argues that the 20th century saw two new forms compete with "industrial machines" of a previous age: "familial machines" reliant on electricity such as consumer durables and "war machines" such as developments in space travel and jets (2007, p. 94-95). After a shift in the 1950s for families and persons to move away from urban centers in favor of a suburban lifestyle (creating a new breed of consumer and at the same time mitigating civilian casualties in the event of enemy bombing campaigns), nexus systems no longer made sense. What make the maintenance of a suburban residence possible are two critical technologies: automobility and electricity. Automobility—made possible through mass manufacturing, the internal combustion engine, fuel distribution and fueling infrastructure, driver training programs, driving rules and etiquette, and road infrastructure—made it possible to live at a greater distance from places of work than was possible with public transportation. Electricity, available in the home and business, enabled the development of nexus-system replacements for what were previously series-system services, from block ice delivery (shift from the ice box to the refrigerator) to live entertainment (live performances to radio programs).

Urry argues that cars are not merely a means of transportation, but are rather "the quintessential manufactured object produced by the leading industrial sectors and the iconic firms within twentieth-century capitalism" (2007, p. 115). The expense of owning, leasing, maintaining, and operating an automobile is significant, and yet, despite the cost, an overwhelming majority of U.S. residents of driving age are licensed to drive, indicating the naturalization of automobility and the importance of being a "driver" in U.S. culture. Further, automobility has changed how movement is conceived through space and time as more personal and flexible, or "person-to-person" more than "place-to-place" as drivers operate on their own schedules to reach destinations of their choosing rather than on the timetables and stations or stops of public transportation (Urry, p. 174).

Urry holds that the current system of automobility is not sustainable, pointing to climate change, fossil fuel supply, policy, fuel systems and construction materials, and argues that moves to "deprivatize" cars and their increased integration with communication systems will reconfigure automobility increasingly as *nexus* rather than *series* systems. Urry proposes two dystopian visions of a "post-car" system: a "regional warlordism" where supplies are fought over and attainable for only a limited few and a "digital panopticon" of complete control and limited mobility. Alternate (brighter) futures would necessitate, in the first place, an energy source so abundant that conditions of scarcity do not become problematic or a society that deemphasizes the individual in terms of privacy, mobility, and choice (David Harvey's imagined world in *Spaces of Hope*, 1990). With these two conditions not reachable in the foreseeable future, a "hybrid" solution is needed that provides for mobility that is both sustainable and personal: a nexus system that drives like a series system.

Before looking to the latest incarnation of such a solution—the electric car—it is necessary to examine a history of development of electrically powered nexus and series transportation systems. I begin with a brief history of electric transportation in order to understand the conditions of the development of the gasoline powered car and, later, a proposed shift to electric automobiles. After presenting the technical and social roadblocks to such development, I will analyze the growth of electric vehicles today in terms of changed social and technical environments, the promises of a better world that they purport, and the new challenges presented by a radically altered system of automobility.

Electric Mobility (Series System)

Histories of electric mobility do not agree on a sole inventor of the electric car, indicating that the 1800s saw a variety of inventors thinking about electric automobility around the world. While some argue that the electric car was initially conceived in the 1830s by Sibrandus Stratingh, a Dutch inventor who created a design for an electromagnetic cart after working on development of steam powered vehicles (Romero, 2009; University of Groningen Website, n.d.), other histories indicate that electric vehicles were also being developed in the 1830s in Scotland (by Robert Anderson) and America, where Thomas Davenport invented a small electric locomotive (Electric Auto Association, n.d.). It was not until the 1890s that a successful electric automobile was invented in the U.S. by Iowan William Morrison, and later in 1897 that electric cars were produced in quantity by Pope Manufacturing in Hartford, CT (Sulzberger, 2004). Sulzburger's history of the electric car reports that while the turn of the century the U.S. was home to a dozen electric car

manufacturers making 28% of U.S. automobiles, a lack of charging infrastructure, voltage issues, and battery maintenance were barriers to the success of the electric car (para. 15).

Powering the vehicle was not the only barrier in electric automobility – there was also the issue of horsepower. Early in the history of automobility the electric car was "the car of choice" but was soon edged out by the gas powered car as "automatic starters, cheaper oil, and mass production" provided advantages for the gasoline powered car (Who Killed the Electric Car, 2006; see also Romero, 2009). Dennis and Urry (2009) explain that part of what motivated the larger switch to gasoline powered cars had to do with the impression that the gas-powered automobile was a "speed machine" after the success of such cars in public road races in France and the U.S. As early adopters of the technology were mainly wealthy males who used the cars as expensive toys, speed and endurance won out over safety and cost.

What limited the electric car then and continues to limit electrically powered vehicles today is the capacity to store generated energy, a challenge overcome in the gasoline powered vehicle through the incorporation of an internal combustion engine, which instead stores fuel that can generate energy on-demand. Overcoming the challenges of storage and distribution is at the foundation of human civilization. Agriculture and the ability to store food to account for future demand made possible the development of urban society, and later developments such as curing, canning, jarring, refrigeration and chemical preservatives have made it possible to store food for longer and transport it across greater distances. Storage of communication in the form of the icon and written word opened up new possibilities for the generation of knowledge: words on paper that could be extended across space and through time were at the heart of Innis' time-biased and space-biased descriptions of cultures – entire cultures defined through storage of something once ephemeral (1951/2008).

The move to electric vehicles hinges completely on questions of storage. With the ability to store energy in the battery, the electric car does not require a live source of energy, instead drawing power from an internal reserve. Interestingly, the battery technology that enables large-capacity energy storage for electric vehicles possible— lithium-ion—is the same technology that makes 8+ hour laptop battery life possible. The car can now be powered in the same way as our other mobile devices. Early on, gas powered vehicles solved this problem by storing fuel which could be burned in an internal combustion engine to create energy required to power the vehicle on an "as needed" basis. The driver, by depressing a lever on the floor of the vehicle, is able to allow gasoline to flow to the engine. This gasoline is then ignited and the expanding gas in the cylinder drives pistons which push a crankshaft and ultimately the driveshaft of the vehicle, propelling it forward (or backward when in reverse). It is no wonder then that the automobile, in its capacity to store copious amounts of mobility-sustaining fuel, facilitated the decentralization of populations in the 1950s and 1960s. The mobile power plant in the automobile enabled a system of distributed power generation and on-demand mobility. Like a horse, draft animal, or steam engine, though, the rider or operator has to "feed" the car.

Moves to decentralize American urban centers have, while extremely lucrative, taken their toll. While the gasoline engine fuels freedom, it also has the negative effects that one associates with distributed processes. Think of it this way: while an electric mobility system gets its energy from a centralized power plant (or plants) where equipment is constantly maintained, monitored, and repaired by experts and engineers, the gasoline-powered mobility system runs off of a collection or mobile power plants operating at varying efficiencies and by individuals with varying levels of mechanical skill. The fuel needed to generate power

also must be distributed, and so rather than a rail line that runs directly from a source to a site where the fuel is consumed, gasoline must be distributed to multiple sites, or stations, where drivers can purchase fuel. While it is not economical to have a gasoline line and pump to every house (as is the case with water), nearly 100 percent of homes in the U.S. are wired for electricity, and so an infrastructure that would support electric automobility has in many ways already entered the home site. The modern electric car attempts to combine the freedom of movement enabled by the internal combustion engine without the deleterious effects of distributed power generation by resolving the necessity of direct contact with a live power source as well as the need for distributed generation. It accomplishes this through the use of advanced battery technology and the development of charging infrastructure. While the electric car is seeing gains in the early 2010s with the release of electric cars by large auto manufacturers including General Motors and Nissan as well as smaller manufacturers Smart and Tesla Motors, it is important to understand this move as one that has progressed in fits and starts.

Electric Mobility (Nexus System)

In order to better understand the origins of today's electric vehicle infrastructures, it is first necessary to look to previous electric transportation infrastructures. By looking at the ways in which electrical and transportation infrastructure were articulated to form the electric streetcar systems that moved millions in the early 20th century, I accomplish two goals. First, I demonstrate that the demise of the electric streetcar was far more complicated than the "buy out and shut down" of electric streetcars as it is often suggested in histories of the electric car. Through an analysis of early 20th century issues of the *Electric Railway Journal*, I will

demonstrate a much more complicated relation between electric and gasoline-powered mobilities that will offer a more nuanced understanding of the decline of electric surface transportation in the US. Second, in looking specifically at the electric streetcar as a nexus system, I demonstrate that the electric car, too, is a nexus system, but that its main advantage is in the elements that make it drive like a series system.

Today's electric car can be seen as having its roots in early electric railways: centrally generated power distributed by specialized infrastructure connected to a larger power grid. In the case of the trolley (and similarly with bumper car amusements), a metal contact has to be in direct connection with a live energy source, and trolley cars themselves have no means of storing power other than in potential energy brought about by gravity (with the car positioned at the top of an incline) or kinetic energy, or momentum (optimized by low friction). The vehicles have no ability to move on their own from a static state without a live external energy source. In addition to requiring a live power source, trolleys demanded a vast amount of specialized infrastructure – tracks and cables and poles – which eventually led to a move away from electric rail as trolley infrastructure needed to be replaced and less expensive alternatives such as electric buses and gasoline-powered buses that had more infrastructure in common with developing automobile transportation became available. Understanding the shift away from the electric streetcar will provide the necessary foundation for understanding a potential shift back to electric transportation, and to do this, I will draw mainly from early 20th century issues of an industry trade journal, *The Electric Railway Journal.*

Before discussing the electric streetcar through an analysis of the *Electric Railway Journal*, it is important to think about the place of the electric streetcar in an already mobile urban environment. In a series of podcasts, online historians Greg Young and Tom Meyers

examine the development of the subway system in New York, beginning with the streetcar and continuing to the present day (2010). They explain that as steam power was not permitted in the heart of the city, streetcars in the 1870s were pulled by horses—more than 40,000 in New York City alone, working 10-12 hours a day—until a horse influenza in 1872 killed thousands of horses across the U.S., crippling transportation and commerce. In the late 1800s, the city imported cable-car technology (powered remotely by steam) from San Francisco, and by the 1890s the horse-rail companies began to consolidate and shift to cable lines. Cable lines were scrapped by the beginning of the 20th century as they were proven to be both expensive and dangerous in comparison to the electrified horseless streetcar (or trolley) developed in 1888 in Richmond, Virginia by Frank Sprague and bought up by Thomas Edison (Young & Myers, 2010).

Young and Meyers explain that this particular solution was not optimal for NYC, as a blizzard during the winter of 1888 damaged many overhead wires, and the city required that overhead lines be buried underground. This obstacle was soon overcome by the installation of underground conduits for powering trolleys in Manhattan, but with fewer restrictions on overhead wires (and a more dispersed population) in Brooklyn, hundreds of lines were developed to serve the area, and Brooklynites were referred to as "Trolley Dodgers," the origin of the local baseball team—the Dodgers—name (Young and Meyers, 2010). In addition to the trolley, New York would see the introduction of the third electrified rail, a monorail and bicycle monorail, and eventually the subway, but not without political resistance. Subways were long delayed by powerful train and trolley interests in New York City politics, not being seriously considered as an alternative until gaining political and popular approval on the basis of job development and overcrowded streets (Young and

Meyers, 2010). Despite issues with companies not wanting to invest, the state of NY passed the Rapid Transit Act in 1894, which organized a commission to create a plan for a comprehensive subway system, which soon replaced elevated trains and trolley cars. The electric streetcar had lost to the subway in New York before the turn of the century, and electric railway and utility companies were determined to keep hold of transportation in the U.S. for as long as possible.

The *Electric Railway Journal*, a trade journal serving electric railway companies and suppliers, provides a clear sense of both changing sets of concerns as well as industries involved in the development of electric streetcars and public transportation more broadly in the early 20th century. Advertisements for track, ties, poles, cable, substations, lubricant, cars, wheels, bearings and brakes dominate issues in the late 1910s and early 1920s, but by the 1930s, advertisements for rubber tires, electrically powered buses, gas-powered coaches made by Mack, the Dodge Brothers, and General Motors as well as advertisements for motor oil and gasoline take up more space in the journal. Issues of concern in the 1910s included electric railway infrastructure development and deployment in cities across the United States, labor relations, public relations and publicity efforts, cooperation with utilities, and traffic regulation. A number of articles in 1916 focused on motor vehicle accidents, with titles such as "The Vehicular Traffic Menace" and "Motor Vehicle Accidents and Traffic Regulation" (No Author, 1916; Windsor, 1916). Throughout 1915 and 1916, a number of articles and news updates focused on the issue of an increasing amount of "jitneys" on the road, and municipal and state efforts to regulate jitney drivers as common carriers through certification, licensure, examination, inspection, and ordinances that drivers be bonded (*Electric Railway Journal*, 1915). Articles about decisions favorable with street car operators were common –

this was a time in which street car operators, as public utilities, enjoyed monopoly conditions that were in many cases protected by state and local governments. Economic competition was not the only concern that electric rail operators had with the automobile – there were also the motorists.

There are a great many articles in the *Electric Railway Journal* that deal with the danger of the motor vehicle, whether gas or electric. H. G. Winsor, a claims investigator and adjustor by trade, wrote an article on "Motor Vehicle Accidents and Traffic Regulation" in October of 1916 in which he provides statistics that demonstrate that, despite increases in traffic, electric railways were able to maintain reasonable accident records. Winsor also conducted an experiment in which three drivers traveled 12 miles in one hour in a densely populated area and between them observed the following persons in potential danger of a car accident: 237 children roller skating; 116 children on bicycles; 98 children playing ball and 74 playing other games; 53 "Nursemaids who wheeled baby carriages"; 91 men who "looked in our direction before crossing streets" and another 152 who only looked after the horn was sounded (p. 875). Besides indicating that roller skating was all the rage with youth in the 1910s, that all women pushing baby carriages are nursemaids, and that only men cross the street, these statistics point to more than 1000 potential victims of a dangerous automobile accident. Agreeing with moves to further restrict who may obtain a license to drive and to set and enforce speed limits, Winsor also cites suggestions for "thank you ma'ams"—depressions in the highway akin to speed bumps or speed tables—as being potentially helpful in getting cars to slow at intersections and railway crossings (p. 876). Other suggestions he discusses involve pedestrian education and prohibiting playing in the street. This is one of many articles discussing the dangers of encroaching automobiles and busses in the 1910s.

The automobile and the jitney continued to be points of contention for electric railway and streetcar companies through the early 1920s, and though some public transit operators were beginning to introduce (or more accurately re-introduce) wireless transportation by means of buses, others remained skeptical. Though some news stories (and advertisers such as White Busses) highlighted the positive attributes of incorporating busses into service, a 6-page article by "Observer" in 1921— "Des Moines Rides Busses and Walks"— makes a strong case against busses in the wake of the discontinuance of electric railway service in Des Moines. Citing a lack of enforcement and changing traffic regulation, the unidentified author writes that "Great numbers of people are walking, and great numbers of women and non-necessity riders are staying at home rather than endure the discomforts, not to say the embarrassments, of the Des Moines motor bus trip" (p. 283). The rest of the article details the way in which the electric railway in Des Moines came to be shut down over increased fares, failed negotiations between the city and the railway company, and the $8,000,000 worth of railway property in the city that was left idle as a result (p. 286-288).

In the following issue, a front page news story titled "How Can Mass Transit Remain a Monopoly" looks at the positive and negative aspects of incorporating automobile service either in combination with or in place of rail service. While the article explains that electric rail services have done the responsible work of moving the public, loosely regulated jitney and bus service threaten all of that ordered, nexus-system motion, particularly because "the development of the automotive vehicle has been so amazingly swift that the law is still a long way from dealing with it in a way that will protect those that have invested most in giving the public what might be called the 'substantial' transportation service" (1921, p. 305). The article suggests that more is needed than anti-jitney ordinances to keep mass transit under the

purview of the electric railway, "the organization with the greatest resources and experience and of proved reliability" (p. 306).

Two years later in 1923, a two page advertisement for White Busses in an issue of the *Electric Railway Journal* presents a different vision of the bus in urban transportation. Shown here as Figure 2, the advertisement consists of a one-page illustration of a White Bus full of businessmen at the curbside in an urban area, as a well-dressed man holding a briefcase next to a woman in a fur coat stand next to the bus. The advertisement explains that a variety of White Busses that have been adopted by electric lines will be on display at the upcoming Electric Railway Association Convention, and the second page of the advertisement explains the benefits of incorporating busses in public transit: "…modern motor bus transportation, carrying on over streets and highways where rails can't go, supplements, feeds and binds together our whole passenger transportation system – to make it adequate and enduring" (p. 121). Positioning the bus as supplementing, not replacing, electric streetcars, the advertisement explains: "where rails end, rubber carries on" (White Busses, p. 121). While the advertisement shows the bus in a well-travelled urban setting, the text suggests that these busses, when owned and operated by the electric railway companies, work to extend service with a personal touch to a moneyed crowd.

Figure 2: Print advertisement for White Busses

1923 issues of the journal include articles on matters including standardization and merchandizing, increasing ridership through more appealing interior design and appointment, increased comfort, and other service-oriented aspects. Contrasted with the attitude toward busses in the 1921 articles, Storrs (1923) explains that the bus is coming to occupy an important place in urban transit, though the tone is still antagonistic. Explaining the difficulties in allowing independent bus operators to serve travelers (including competition on heavily travelled routes), Storrs suggests that coordination can only occur if there is no competition between services, with bus routes serving distant populations or rail routes that have been abandoned. He suggests that in some cases, bus routes could operate during the day to service routes "entirely impossible by rail," making clear that if busses are to be cooperative with electric rail, they must steer clear of competition with rail (p. 590).

Storrs' article is one of many in the issue that addresses the incorporation of and/or cooperation with busses. D. W. Pontius, Vice-President and General Manager of the Pacific Electric Railway in Los Angeles, explains in "Co-ordination of Trolley and Bus in California" that competing service is not tenable for the railway company, and that with moves to provide railway operators with more of the transit market, companies have been able to incorporate their own bus service in efforts to provide "trackless transportation" along with existing railway services. Throughout the article, Pontius works to show that bus services operated by rail companies interested in serving the public are superior to that of bus-operators who are essentially looking to make a quick buck. Turning specifically to Los Angeles, he writes that "Probably the hardest battle ever sustained by electric transportation companies to retain their right to serve a city, to repel an alien interest, and to protect itself from unwarranted and unfair competition was made in Los Angeles recently" where an application was made for a bus service to run parallel to existing rail service that would work to "skim off the cream of traffic, and not to develop any new territory" (p. 598). The electric railways carried out a public education campaign through the news and door-to-door, and were able to ensure continued control over public transit, operating their own bus routes and continuing to invest in "trackless transportation" even if they were operating those lines at a loss and favoring regulation of bus service. Pontius writes: "the problem of the electric railways is not to put the busses and trucks out of business but to see that they are used in districts not adequately served by rail transportation" and suggests that operators add bus services to hold onto their own business (p. 599).

A report of the proceedings of the American Electric Railway Association from the 1923 convention compiled by Executive Secretary J. W. Welsh focuses on a variety of

topics, including finances, government relations, trackless transportation and highway construction. Specifically regarding trackless transportation, Welsh reports that railways adopting bus service nearly doubled from 44 to 95 companies, and the busses more than tripled from 300 to 925 (1923, p. 619). Welsh also reports that "The menace of the jitney, although still present, has grown less" partially due to the more organized bus service now provided, in part, by electric rail companies (p. 619). Reading over many technical reports and speaking from personal experience, the committee draws two main conclusions: 1) the electric rail system is still at the core of providing transportation to, from, within and between cities; 2) the bus is necessary to supplement, feed, and extend these core services. From this, the report looks at motor vehicle regulation as it pertains to common carrier services as well as the lack of clarity in descriptions of projected costs for building and maintaining roads and highways. "The members of the committee are convinced that the motor bus has come to stay. It is a business proposition, not a theory" (p.620).

The journal also contains an article written by H. W. Alden, President of the Society for Automotive Engineers, concerning the report compiled by the Committee on Bus Operation. Alden suggests that the results presented would be more helpful if they would have considered bus operation outside of the electric railway context and looked more specifically at different kinds of equipment and other factors not considered by the committee. He cites the publishers for the journal *Bus Transportation* as well as individuals at Yellow Coach Company and General Motors as being helpful in preparing his comments. He writes "It is gratifying to us motor people, however, that in spite of the rather gloomy picture painted, the consensus of opinion among your operators seems to be that the motor bus is here to stay" (1923, p. 602). 1923 issues reflected a continued focus on the dangers

associated with automobile transportation, including articles on the transformation that a commuter undergoes when he becomes a driver. L. F. Wynne, a General Claim Agent for the Georgia Railway and Power Company writes: "This tendency towards recklessness on the part of automobile drivers is, I suppose, but a manifestation of the trend of the times; an outgrowth of our vaunted hustle and speed" (p. 689). Discussing the difference between the well-trained engineer, confined to the tracks, and the automobilist, who often acts with disregard to the safety of others, Wynne suggests examination and yearly licensure for auto drivers. Pages earlier, Ralph Emerson, General Manager of Cleveland Railway, explains the safety training that rail operators must go through in order to demonstrate a concerted effort to reduce accidents on the part of public transit, and suggests that the more dangerous drivers should enroll in compulsory driver education programs. Emerson notes that the streetcar operator is in a difficult position, however: he must both operate safely as well as quickly in order to ensure continued relevancy of the street car as a mode of transport. One potential solution he suggests is "the separation of traffic by creating 'streetcar streets' and 'automobile boulevards'" (p. 683). Other issues that he raises are concerns with right-of-way as well as parking on main thoroughfares, particularly during rush hour, as well as enforcement of traffic law.

By 1930, the *Electric Railway Journal* reflects a different take on automobile and bus transportation: multi-page spreads for motor coaches from manufacturers such as Dodge Brothers, Mack, and Yellow Coaches as well as General Electric's Gas-Electric Busses accompany those for tires, motor oil, and gasoline. Some advertisements and articles focused on advances in signaling systems for rapid transit and larger features about the coordination for the overall transportation system in a given urban area. Jitneys, much discussed in earlier

issues of the journal, are absent, now replaced by articles and stories about taxi-cabs and taxi-services: the gasoline-powered motor now had a place in the *Electric Railway Journal*.

A story about the development of bus service in Patterson, New Jersey in a 1930 issue discusses the increased flexibility of bus service in transporting passengers to and from work, and explains that jitney service picked up during the World War and workers (particularly female workers) grew accustomed to being dropped off right at work, providing faster and more convenient service at a lower cost than street car service. This combined with increased car ownership (which increased road congestion) contributed to the public transit system being less profitable. Electric rail companies slowly replaced streetcars with busses, which had the advantage of eliminating the need to replace aging rail infrastructure and employing men to switch tracks at crossings as well as enabling the public transit service to navigate narrow streets and make special trips to mills on a more flexible schedule (Busses Replace Cars, 1930, pp. 315-317).

An article concerning the usefulness of the bus in electric railway operations authored by Carl Stocks (1930), Editor of *Bus Transportation*, details the many advantages of bus transportation, including the range of sizes in which busses are available, the reduced cost of operation due to lack of specialized track infrastructure, the easy ride that rubber tires enable for passengers and increases in power and speed with the move from the four to the six cylinder engine. He does note that there is room for improvement in bus design however, citing the smell of exhaust that often fills the cabin and the heavy materials that busses are often made of that drag on performance. Other articles in this volume look specifically to the advantages of the gas propelled bus and coordinating public transportation with the "taxi-cab," a much more organized service than the jitneys discussed in years previous. Bus

advertisements, sometimes four pages long, fill the magazine, a testament to changing transportation needs and possibilities. An advertisement for Yellow Coaches touts the largest order in history for coaches from a motor carrier—300—by Greyhound buses (Yellow Coach, 1930). By 1930, the *Electric Railway Journal* has become less about electric railways than transportation, and transportation has clearly moved beyond the electric railway to more flexible modes of public transit.

In many ways, we might understand the move to gasoline-powered vehicles as a move to wireless transportation. With the limitations of trolleys proven by the 1930s and battery technology for electrically powered vehicles limited, gasoline powered busses demonstrated clear advantages in power, speed, infrastructure cost, and flexibility in terms of routes and time. Gasoline enabled a shift to wireless mobility. With gasoline prevalent in the U.S., an entire industry boomed around the convenience of the bus at the same time that the automobile began to boom. The purpose of this history is to demonstrate that, rather than thinking of the demise of the trolley as an effort on the part of the automotive industry to sell more passenger cars, a broader view shows that the wired electric streetcar was already losing favor in the early 20th century to the bus, and that electric railways fought tooth and nail to maintain a hold on urban transportation, even if it meant securing their own fleets of gasoline powered busses.

Who Killed the Electric Car?

Citing smog and global warming as a major public health crisis resulting from the gasoline powered cars, *Who Killed the Electric Car* focuses on early moves to deploy the electric car in California, beginning with passage of the "Zero Emission Vehicle Mandate"

(ZEM) by the California Air Resources Board (CARB) in 1990 that required auto manufacturers selling cars in California to also make available zero-emissions vehicles. While many car manufacturers complied with the mandate by converting gas powered cars to electric cars, at the center of this documentary is the EV1 produced by General Motors and marketed by Saturn, the first electric car from a major automaker since the early days of car manufacturing.

As major pushback from the oil industry and lack of cooperation from the auto industry hampered the efforts of electric vehicle acceptance and deployment, CARB accepted a negotiation on the ZEV mandate to require manufacturers only to supply the demand for electric cars, resulting in moves to kill demand for electrically powered vehicles through lukewarm advertising, long application processes, and un-selling potential leases until a point came where General Motors could begin to shut down dealerships marketing electric cars. Since electric vehicles were leased without the option to buy, automakers were able to quietly get these cars off of the road by not allowing drivers to renew at the end of their lease or have the option to buy the vehicles. The documentary shows the way in which reclaimed EV1s were collected in holding areas before being ultimately taken to General Motors' proving grounds in Mesa, Arizona for destruction, despite statements from their communications representative saying that the cars would be used for research and testing, display, driven by General Motors engineers or dismantled and recycled. Activists began to follow truckloads of reclaimed electric cars by other automakers such as Honda and Toyota only to find them being crushed and shredded. The documentary locates one EV1 at the Peterson Automotive Museum in Los Angeles CA, though it has been disabled and stored among a range of other relics in an underground vault.

In an effort to assign blame throughout the documentary, seven potential culprits are examined, including car companies, oil interests, battery manufacturers, the California Air Resource Board (CARB), consumers, the government, and the hydrogen fuel cell. All but one—battery companies—were found guilty in the death of the electric car. Here I focus on three culprits—car companies, oil companies, and the government—discussing consumers, CARB, and the hydrogen fuel cell as they are connected to what I identify as the main culprits (failures on the part of consumers and CARB as well as the over-hyped hydrogen fuel cell largely derived from auto manufacturing, oil interests, and government actions).

First, car companies have an antagonistic history with electrically powered mobility. As the documentary notes, the red trolleys that were designed initially as a means of using energy during a point of low consumption (when individuals are travelling to and from work, and so using electricity at neither) were bought up by General Motors and shut down in an effort to reduce alternatives to automobile transportation and increasing a potential pool of automobile consumers. Though this may be the case, when situated in the longer history of relation between the electric streetcar companies and automobile manufacturers, it can be understood as reactive and not preemptive. The documentary explains that while CARB mandated the manufacture of the electric car through its Zero Emissions Vehicle Program, automobile manufacturers were reluctant to comply, seeing little profit in the short term in electric vehicles (EVs), much of which can be attributed to differences in gas powered and EV repair and maintenance (Deeter and Paine, 2006). Without an internal combustion engine, supplies such as oil and filters are not needed, which means losses in service and parts revenue. A mechanic interviewed in the documentary explains that servicing the EV1 essentially just meant filling the washer fluid and rotating the tires. With no short term profits

in the electric car, the documentary explains that General Motors, which bought Hummer in almost the same stroke as they shut down production on the EV1, focused instead on the SUV market. The government seemed to support such a move, with tax breaks for electric vehicles in 2002 capping out at $4,000, while a year later, tax breaks for vehicles over 3 tons topped out at $100,000 (many pick-up trucks qualified as did some work and passenger vans, but so did SUV models such as the Cadillac Escalade, Dodge Durango, Ford Expedition, and Hummer H1 and H2).

Graham and Thrift (2007) explain that repair and maintenance are often overlooked when discussing systems of automobility. Examining road-side repair, road repair, and automobile accidents as part of a larger argument about the importance of processes of repair and maintenance, they work to "surface the invisible work" that Star alludes to in her article "The ethnography of infrastructure" (1999). Here I am interested in following the money involved in that work to help make the case that the maintenance and repair market—a combination of a service and manufacturing industry—played a large role in the decision not to advance electric car technologies in the 1990s. The U.S. Bureau of Labor Statistics reports that in 2008, more than 763,000 workers were employed as automotive service technicians and mechanics, a number projected to increase to nearly 800,000 by 2018 (U.S. Bureau of Labor Statistics, 2011). Automobile repair and maintenance services constitute a more than $85 billion industry in the U.S. alone (U.S. Census Bureau, 2009b) and a shift to electric vehicles with fewer moving parts (which are less likely to break down) would significantly reduce profits from oil changes, filter replacements, and parts sales, many of which sustain small repair shops and dealer service locations across the United States. Understandably, auto and parts manufacturers are reluctant to give up on this profitable aspect of the industry.

Lack of manufacturer interest in the electric car had a direct impact on consumer demand for EVs. While the documentary argues that the consumers were partly to blame for not showing significant interest in the promise of the electric car, it also highlights the lackluster presentation of Saturn's EV1. In an age where so much is actively sold to consumers, it is hard to blame the majority of drivers for not proactively seeking out what was essentially invisible to them in a barrage of (well-appointed and powerful) gasoline-powered cars. Indeed, it could be argued that the decision for tasking a small and newly formed division with launching the EV1 was a further effort to deter interest in the vehicle. The film explains that auto manufacturers harbored resentment about being told what to do by CARB, presenting a confidential memo that indicates that the American Automobile Manufacturers Association hired a public relations firm to work towards repealing the Zero Emissions Vehicle mandate through grassroots campaigning. Automobile industry efforts to fight the ZEM are obvious, but are yet dwarfed by the efforts of a larger industry with more to lose – the oil industry.

Oil interests have been a prized target of blame for everything from greenhouse emissions to low fuel efficiency and war. While calls to move to renewable energy sources are often supported by evidence that fossil fuel supply is limited, those with business in supply, extraction process, equipment, refineries and patents for petrol-fueled machinery have a stake in ensuring that petrol-based products will continue to be in high demand. As supply dwindles and demand remains high, the estimated $100 trillion of oil left on Earth could become even more valuable (Deeter & Paine, 2006). The documentary also uncovers the fact that Californians Against Utility Company Abuse, a consumer organization that fought the implementation of charging stations, was funded by oil companies. Oil companies

also took out newspaper editorials that called the environmental benefits of electric vehicles into question, though despite being potentially powered by electricity from coal-fired plants, electric vehicles were still found to be more efficient and cleaner than gasoline powered vehicles.

In fact, part of what absolves the battery companies of guilt, according to Deeter & Paine, is the involvement of oil companies in blocking development of new battery technology. *Who Killed the Electric Car* includes multiple segments with Stan Oshinski, developer of an advanced battery (Ovonic) that was bought by General Motors and later purchased by Texaco, who effectively crushed the technology (Deeter & Paine, 2006). Much of the fault of the death of the electric car seems to link back to the oil industry, which saw the technology as a threat to short-term profit rather than a long-term solution for post-peak oil automobility.

The third party that I will discuss here is the U.S. Government. Describing a government that has not spurred industry to make cars more fuel efficient (in part due to pressure from oil interests), *Who Killed the Electric Car* points to a history of poor energy policy, citing the Reagan Administration's work to undo much of the energy policy of the Carter Administration through moves to deregulate energy, to OPEC's lowered prices that made alternative fuels less attractive. The documentary also notes that though a hybrid vehicle program was launched during the Clinton Administration, it was abandoned in the Bush years (though it spurred foreign automakers to develop hybrid cars) partially due to multiple ties to oil and auto manufacturing in the G. W. Bush White House, the same administration that would eventually join General Motors and other automakers in a lawsuit against CARB while simultaneously pushing the development of hydrogen fuel cell vehicles

(Deeter & Paine, 2006). The film illustrates how the hydrogen fuel cell was positioned as the alternative of choice in the early 2000s, showing clips of the newly elected Governor Schwarzenegger driving a hydrogen fuel cell powered Hummer concept vehicle used in a campaign to support "a hydrogen highway to take us to the environmental future" (Schwarzenegger, quoted in Deeter & Paine, 2006). In an April 24 2003 hearing of the CARB, under the leadership of fuel-cell advocate Alan Lloyd and with pressure from the auto industry, oil industry, and the government, the board voted to end the EV mandate.

The roadblocks to wide-scale deployment of hydrogen fuel cell technology are many and encompass issues ranging from hydrogen extraction and fueling infrastructure to cost, range, and safety. Because there are no stores of hydrogen that can be easily mined or collected, hydrogen has to be obtained through processes that rely on an external power sources such as electrolysis or steam reforming, in which a hydrogen carrier (usually a fossil fuel) is broken down and the H_2 is extracted (National Energy Education Development Project, 2011). These processes take more energy than the hydrogen ultimately provides, with current technology. In the fuel cell, hydrogen is not a fuel, but a storage mechanism (though hydrogen is the ultimate fuel for fusion, as with the Sun, this cannot be done inside a car). A second major roadblock on the hydrogen highway is the issue of limited access to fueling stations. With no idea as to when the hydrogen fuel-cell vehicles will be on the market, hydrogen infrastructure build-out has been slow. This story is complicated by a third point: the limited range of a hydrogen fuel-cell vehicle. In contrast to the electric vehicle, where limited infrastructure is less problematic due to the ubiquity of electrical infrastructure that can be tapped at relatively low cost at home, work, and public charging stations, hydrogen fueling requires separate production, storage, delivery, and pumping. In some

senses, these limitations are what gave hydrogen an advantage in the early 2000s: hydrogen fueling infrastructure is similar enough to that of petrol-based products for BP to fit at an existing gasoline fueling station to also provide hydrogen fuel as early as 2004 (BP, 2004). As of 2009 there were only 120 hydrogen fueling stations in the United States, a figure which falls short of California's "Hydrogen Highway" targets of 150-200 stations in California alone by 2010 (Sullivan, 2009).

Joseph Romm, former Acting Assistant Secretary of the U.S. Department of Energy and author of *The Hype About Hydrogen* (2004) explains that there are five major roadblocks that must be surpassed before a hydrogen fuel cell car can be successful: 1) as of the making of *Who Killed the Electric Car,* fuel cell cars cost more than $1,000,000; 2) current hydrogen fuel cell cars have range limitations; 3) hydrogen fuel is 3 to 4 times more expensive than gasoline; 4) there is a lack of fueling infrastructure; and 5) competing technologies (such as hybrid, plug-in hybrid, and electric vehicles) must not improve, as even slight improvements would make these competing technologies vastly superior to the hydrogen car (Deeter & Paine, 2006). According to Romm (2004), hydrogen (a gas) requires more than 3,000 times more space by volume than its equivalent in gasoline, which will also pose challenges in fueling and distribution infrastructure (p. 20). In some senses, the story of the hydrogen fuel cell is similar to that of the ethanol bubble in the late 2000s. As gas prices rose, blending petroleum fuel with ethanol was positioned as a solution that would be environmentally friendly (ethanol burns cleaner than gasoline), good for farmers (a broader market for crops such as corn), and less expensive than oil, which spiked to 134.44 a barrel in July 2008, causing the national average gasoline price to soar to more than $4.00 a gallon (EIA, 2011d).

Despite environmental benefits, as oil prices fell, ethanol became more expensive than gas, and some ethanol plants constructed based on predictions that oil prices would continue to rise operated at a loss. Some were unable to pay for equipment and construction costs, mandatory testing, and staffing, and went bankrupt (a further complication of the move to ethanol was the resulting inflation of grain prices, which caused food riots in developing countries around the world). Combined with soaring prices of corn, the ethanol market took a hit in early 2008 causing some to claim that the ethanol bubble had popped (Walsh, 2008), but according to the Renewable Fuels Association [RFA], as of January 2011 there were 204 operating plants, up from 139 in January 2008 (RFA, 2011b). The site also indicates that though production and demand for ethanol is on the rise, the U.S. has been steadily importing ethanol from foreign countries to meet U.S. demand. Interestingly, ethanol hitched their wagon to the hydrogen fuel-cell star early on, as is detailed in a 2002 whitepaper written for the Renewable Fuels Association (RFA): "Ethanol & Fuel Cells: Converging Paths of Opportunity" (Bentley & Derby, 2002). The lead-in on the website explains that the paper "presents a vision of how ethanol and fuel cells can be combined to create significant synergy, reaching markets and bringing benefits that are not achievable with any other fuel or with any other power technology" (RFA 2011a). Though the ethanol market has rebounded from a period of uncertainty, the failure of the hydrogen vehicle to become a success may have contributed to a downswing in the ethanol market.

While progressive energy policy and fuel efficiency have seen gains under the Obama Administration, much has yet to be accomplished. As a case in point, the Cash for Clunkers Program (Car Allowance Rebate System), though sold as a "green" program, was first and foremost a stimulus program for the ailing auto industry. If a documentary titled "Who Killed

the Hydrogen Fuel Cell Car" is ever to be made, it will surely feature the Obama Administration as one of the liable parties, as the 2010 Department of Energy (DOE) budget resulted in a $100 million dollar cut for the hydrogen fuel cell program (now $68 million) and a change in name: it is now simply "fuel cell technologies" (Biello, 2009, para. 1).

In 2006, though it closes by talking about small startup companies and Do It Yourself (DIY) projects and a second life in the form of a plug-in hybrid (such as the Chevrolet Volt), the film did not predict the return and growth of the electric car that is taking place today. The government has by and large failed to spur development of alternative automobilities, and increased consumer interest in electric vehicles stems rather from moves to an increasingly networked lifestyle as well as concerns about fluctuating gas prices and global warming. With what are now clear market opportunities for electric vehicles, small startups such as Tesla Motors and Better Place as well as larger auto manufacturers have begun a second wave of electric car development in the U.S. and abroad. I will next examine the "reboot" of the electric car, focusing on the success of Better Place and extending my analysis to EVs developed by larger auto manufacturers.

Resurgence of the Electric Car

In contrast to ideas of "militarized urbanism" discussed by Graham (2010) and the role of the Jeep, and later the Hummer, which Packer (2007) argues represent American military prowess, the broad selection of available and prototype electric cars are portrayed as light, energy-sipping, and environmentally friendly. The electric car (and arguably most hybrids and subcompact high fuel efficiency subcompacts recently introduced to the U.S. market) are less machines of war than they are a connection point, a hub, or—as is the case

with the Nissan Cube—a "mobile device." The car is no longer a command station, serving instead as a mobile media center that will synch with your smart phone, plug into your smart grid, and be the most mobile part of your smart life. The Better Place solution is perhaps best understood as a *platform*, or a support infrastructure that enables a variety of *screening technologies* to intersect, operate, and transform both cabin space and the driving experience. Unlike the rugged individualism and battlefield-readiness manufacturers used to market sports utility vehicles and trucks to consumers in an era of cheaper gasoline, the electric car is equipped with a sense of environmental responsibility, entertainment, and connectivity.

The electric solution takes advantage of an infrastructural condition that Graham and Marvin term *splintering urbanism*: a move away from the modern infrastructural ideal where municipal and state governments are charged with the provision of unified infrastructure and private industry. Instead, it takes advantage of the splintering of these services brought on by shifts to privatization of public works and network infrastructure. While the splintering or privatization of infrastructure is often seen as having negative social effects, in this case, a company has taken advantage of such an environment in order to deploy an innovative environmental solution that was not possible in the previous arrangement. Through the deterritorialization of the modern infrastructural ideal (see Graham & Marvin 2001), Better Place is able to articulate an environmental, convenient, and (presumably) profitable solution to a stagnant petrol-based mobility market. I will next focus on Better Place's "solution" in order to understand the nature of what is being provided. They are not providing vehicles, nor power, nor a system or even a separate infrastructure. How then is the company making the world a *better place*?

Launched in 2007, Better Place has been the subject of much buzz over the past few years as a viable electric car solution. Preparing to launch the first nine of forty battery swapping stations as part of a nation-wide charging infrastructure in Israel in late 2011, the company is working toward providing integrated battery swapping, home, and public charging solutions. Rather than leasing vehicles, the company's strategy involves drivers purchasing a car and then signing up for a membership which includes installation of a private charging station, access to their network of charge spots and switching stations, batteries, customer support, energy and in-car energy management and navigation software (Better Place, 2011b).

Better Place refers to itself as "the global provider of electric vehicle networks and services," clearly distinguishing their business as the work of articulating infrastructure and not of manufacturing vehicles (Better Place, 2011a). According to the website, the solution comprises: 1) batteries; 2) switch stations; 3) charging infrastructure; 4) driver services; 5) network software; and 6) the provision of standards. I argue that these components, marketed as part of a unified "solution" are best understood in terms of a platform[2]. Better Place is poised to succeed where other EV initiatives have failed due precisely to this platform approach: the company is not providing vehicles or power, but a proprietary grid.

Before discussing the solution, it is important to first understand the problem, or as the Better Place website frames it, the "opportunity" through four main areas: energy, environment, economics, and cars. At the intersection of a dwindling oil supply, and a rise in the growth of renewable energy, the website explains that moving from a petrol-based

[2] Platform as previously defined in this work as a specific articulation of existing infrastructure, devices, and software designed to facilitate further development and deployment of products, services, and infrastructure.

transportation system to an electric one based on renewables would be mutually beneficial. First, when combined with an informationalized grid, an electric vehicle system (their term) will make use of underutilized electricity; second, it can level out grid use; and third, due to increased efficiency, it can "reduce the overall burden on energy resources" (Better Place, 2011a). Environment is also discussed as part of the opportunity, with fossil fuels contributing to deleterious environmental effects and needs to increase efficiency and move away from fossil fuels. Economics are discussed in terms of market opportunities in renewable energy and potentially lower transportation costs. Electric cars, the last opportunity area, are "becoming inevitable" and the site explains that Better Place is working with the Renault-Nissan Alliance and is in talks with other manufacturers to build partnerships. In comparison to the unimpressive marketing for the EV1, Better Place positions electric vehicles as distinctive and inexpensive to maintain and that "in the coming decade, EVs will be at the center of mainstream personal transportation" (Better Place, 2011a). Given this opportunity, Better Place has positioned itself at the nexus of a variety of infrastructures, as a platform rather than an infrastructure or system.

The solution includes a variety of components, and here I will look specifically to those that they highlight on their website: Batteries, Switching Stations, Charging, Driver Services, Network Software, and Standards (Better Place, 2011a). After reviewing the content of these sections in detail, I explore how Better Place poses informationalized infrastructure as central in an emerging "smart" technological sublime. After identifying the features of this emerging technological sublime, I will discuss a number of features of electric and networked mobility that remain largely unaddressed, including environmental impacts, safety concerns, and security risks.

Better Place's solution is one in which a driver purchases or leases a vehicle and then subscribes to an energy service. Batteries, owned by the company, would be stored in the drivers' vehicle or at the company's battery switching stations. The company currently has a partnership with French auto manufacturer Renault, who has built an electric vehicle that is compatible with their automated battery switching process, perhaps the most unique part of the Better Place solution. A press release on the site explains that:

> Customers simply swipe their membership card, which authenticates the car and subscription via the Operations Center to activate the switch. The rest of the process is automated, similar to going through a car wash, so the driver never has to leave the car. In less than five minutes, a robotic arm removes the depleted battery and replaces it with a full one and the driver is back on the road. (Better Place, 2011b, para. 17)

Also included in a subscription to this energy service is the installation of a charge spot in the user's home or workplace, and access to charging points located at various public locations. As with the battery switching stations, drivers would swipe a membership card and charging would begin. The combination of charge points and switching stations enables drivers to participate in the developing energy market afforded by the smart grid, buying and selling power based on price and demand, but also the convenience of battery switching which makes the process of getting more energy for the car take about as long as pumping a tank of gas. While multiple options for recharging the car make the solution attractive for drivers who do not want the switch to an electric car to change their experience of fueling it radically, what is perhaps most relevant to the present analysis is the integration of information into the process, both in terms of driver services and network software.

Better Place gives the impression that the integration of information is a central and important component in their solution, and one that will make the move to an electric car an

attractive one for tech-savvy drivers. On the EV (electric vehicle) Driver Services page of their site, they write:

> Advanced in-car software and telematics systems are bringing more and more technology into cars and making them easier and better to use. These types of systems have traditionally been expensive options, often secondary to other factors in the decision to buy internal combustion vehicles. In EVs, telematics become much more important and are considered to be one of the primary differentiators that consumers will care about.

This section of the site then includes a number of pictures that show the types of things that these systems will be able to do: locate charge stations for the driver and provide navigation services, guide drivers through the battery switch stations, link to smart phones via applications that show the battery charge status, and keep drivers apprised of the status of batteries and proximity of charging locations on a constant basis.

A video on the site shows a driver, Henry, checking his battery while drinking a morning cup of coffee or tea, unplugging the vehicle and dropping his daughter off at school, driving to work, parking and picking a cord up off of his passenger seat and plugging in again. As he makes a trip out to visit a construction site, his display alerts him to traffic and reroutes him, and on his way back the display alerts him that he will need to recharge, and presents the options of either plugging in or switching. As his nearly spent battery is swapped for a charged one, he calls his wife on the phone:

> Wife: “Hey!”
> Henry: “Guess where I am? Switch Station!”
> Wife: “Really, it’s been a while”
> Henry: “Yeah, I had to go to the site today”
> Wife: “Oh, are you going to be home late?”
> Henry: “I’ll be done here in like, two minutes. See you shortly”

When Henry parks in the driveway, he plugs in his car and walks into his house to be greeted by his daughter and pregnant wife, but the last image that we see before the company logo is one of a smart phone with a Better Place application indicating the battery is at full charge (Figure 3).

Figure 3: Charge complete: Still image from Better Place promotional video

While the video suggests an interesting relation between home, work, travel and communication in an electrically powered automobile experience, the Better Place solution also comprises dimensions that go beyond the driver to solidify this platform as one that would be preferred by utilities and public planners (ev Network software) and manufacturers (Standards). Better Place's ev Network Software enables the company to "monitor all the batteries in the network (residing inside vehicles and in switch stations), aggregating data on each battery's state of charge and anticipated energy demand" in real-time, enabling batteries plugged in to their network to serve as distributed storage for utilities (Better Place, 2011a). This potential practice—leveraging car batteries as distributed storage—represents the flip

side of the electric streetcar in the early 1900s: while then electric mobility was a place for energy to *go* in times of low energy use, this solution represents a place for energy to *come from* during high use, representing more than just a return to a nexus system for mobility, but an intensification of it.

With standards, the company works to advance electric mobility more largely, and while battery switch stations remain tied to the specific vehicles with which Better Place has developed partnerships, the charging spots (which have been built to international standards) could serve all electric cars. The organization is working with international bodies such as the ISO and IEC to standardize charging connectors, striving to keep their network open to the widest possible set of electric vehicle drivers to both maximize the potential market for their solution and to position their company as a global leader. Standards often have a power that even trumps the force of law, as material investment in infrastructure built on an accepted set of standards contributes to "lock-in:" once a certain amount of money is invested into doing things in a particular way, and this articulation gains momentum, it is difficult to change or reverse the process: consider, for example, the money invested in broadcasting in both radio and television. The spectrum can be used in many different ways, and the advent of digital technologies increases the range of possibilities for the ether, and yet after the move to digital television in the U.S., traditional broadcasting was retained, and merely "rebooted" in a digital format. The decisions made in the regulation and standards setting in early radio—before television, the widespread adoption of automobiles, and World War II—continue to shape the ways in which the airwaves are used (Streeter, 1996). With a focus on standards, Better Place is working to ensure that their solution will have purchase with regulators and be purchased by electric automobile drivers the all over the world.

Better Place has focused on articulating transportation, communication, and electrical infrastructures in a way that puts their organization at the center of negotiating consumption, information flows, movement, storage, and standards in electric automobility. Further, in creating a platform that is not unique to a specific geography, the company is also positioned to profit from the use of their platform globally by manufacturers, drivers, and utilities. With gas prices in the U.S. peaking at over $4.00 a gallon in 2008 and climbing back toward that number in April 2011, the economic climate is ripe for electrically powered automobility. As the climate in the Middle East continues to destabilize, alternative energy sources are critical, especially for Israel, home to Better Place and the site of the company's first nation-wide deployment. While the geography and culture of the U.S. is perhaps a long way from an electrically powered automobility system, increasing gas prices and environmental concerns make for the beginnings of a receptive market. What pushes possibility to potential, however, is an emerging cultural climate in the U.S.: the *smart sublime*.

Demystifying the Smart Sublime: Challenges in Electric Mobility

So far we have explored the new borders of informationalized infrastructure via electric mobility, making a point to avoid the failings of the "politically and morally irresponsible" research that contributed to largely uncritical perspective on information networks (Carey, 2005, p. 445). First, this analysis has been grounded in larger historical trajectories of the infrastructures of automobility and electric transportation. Second, by paying particular attention to the coevolution of electric automobility with other networks, technologies, and systems, particularly the role of information technology, the analysis has not centered on electric car technology in a vacuum. Lastly, by examining larger contexts in

which informationalization—a practice of layering information technologies with other systems and infrastructures—plays a role, electric automobility has here been explored in a way that speaks to larger cultural, political, and economic contexts. In an effort to describe and explain the smart sublime, this analysis takes the integration of automobility, electricity, and information technology as an object of analysis, working towards an understanding of how beliefs about technology come to shape both understandings of infrastructure and the organization of infrastructure itself. I next discuss some of the drawbacks of such a move to ask whether or not it is, more broadly, a truly smart solution. While the advertising campaigns (Better Place) play on tropes associated with Carey and Quirk's technological sublime, here I identify a few factors that need to be considered in the move to an electric car system that remain conveniently outside of the frame, including issues of mobility on-demand, environmental justice, and dependency on foreign metals.

Mobility On-Demand

> But perhaps the biggest question for electric vehicles (and hydrogen cars as well) relates to infrastructure. How and where will drivers be able to recharge their all-important lithium-ion batteries, particularly if those drivers venture far from home? In most cases, this means they plan to drive farther than the 160 to 240 kilometers they'll get from a fully charged battery. (Greenemeier, 2009, para.4)

In identifying growth inhibitors to electric automobility in a 2009 press release, Price Waterhouse Coopers suggested that the success of the electric car is tied to battery technology, infrastructure deployment, and the space and time required for charging as well as challenges in pricing electricity consumption: all issues that relate to the ability for the electric car to drive like a gas-powered one (2009). Manufacturers of electric vehicles want more than anything to address notions of continued on-demand mobility and consumer

convenience. Slack and Wise (2005) explain that the notion of convenience has shifted from what is suitable to what is comfortable, leading to a general state of perpetual dissatisfaction. In the present post-peak oil environment, it is convenient that individual mobility can be driven by virtually any power source—from fossil fuels to renewable sources such as wind and solar energy—without redesigning the car for each new fuel. It is also convenient (in the second sense) that transportation and information networks are linked, making vehicles accessible from a cellular phone where the driver can check battery status before getting into the car, and then from the car locate the nearest charging or battery swap station.

Questions of power and efficiency are major points of discussion in the move to electric vehicles: in other words, what kind of mobility will electric cars permit, and will it be fitting in terms of the power that electric cars will be able to provide? The electric Ford Focus, due for release in 2011, will have a 100-mile range and is powered by a lithium ion battery and a liquid cooling system that would charge in 6 hours from a home outlet (Biello, 2010). The Nissan Leaf also has a range of 100 miles, and is capable of speeds up to 90mph (Nissan, 2011). The Chevrolet Volt, also featured as an electric option, can reach speeds of up to 100mph and combats "range anxiety" by equipping the car with an on-board gasoline-powered generator that would supply additional electric energy to the vehicle if stopping for a charge is inconvenient or not possible (Chevrolet, 2011). In fact, General Motors sought to trademark "range anxiety" in fall of 2010 (Ramsey, 2010). Tesla Motors seems to solve for both decreased performance and limited range with their fully electric Roadster, which gets 245 miles per charge and gets to 60mph in 3.7 seconds with a top speed of 125 mph, though at a cost of more than $100,000 it will likely not compete with the Volt, Leaf, or Electric Focus (Tesla Motors, 2011).

Anxiety over whether or not the electric vehicles geared toward the average commuter can rocket to 100 or more miles per hour with solid foot to the floor may seem ludicrous to the "smart" consumer, but considering the important role of the car as driving machine in American culture, this is understandable (you never know when you might need to pass someone, after all). There are indications that the power available at the push of a pedal may not be as important a concern moving forward, however, particularly as new ideas about what sustainable and affordable automobility will look like emerge. Responding to Obama Administration efforts in the Department of Transportation and Environmental Protection Agency to raise fuel efficiency to 47-62 mpg, *Scientific American* writer Saqib Rahim asks whether or not Americans will be willing to accept reductions in vehicle size and performance, noting an increased interest in crossovers in the American market that sacrifice weight for fuel efficiency while maintaining equitable levels of performance (Rahim & Climatewire, 2010). Taken together with the potentials of electric mobility, drivers will have to balance power (range and performance), size, and price, essentially facing them with this choice: fast, good, cheap (pick two).

Even as we think about new configurations of the car and speed, size, and affordability, the move to pure electric vehicles (PEVs) raises new questions about how we would gauge that new economy of energy use in terms of time (kilowatt hours) rather than space (gallons of fuel). Moyer, a writer for *Scientific American* (October 26, 2010) explains that in a transitional period, the U.S. Environmental Protection Agency has adopted MPGe (e for equivalent) that is "a conversion factor that measures the electricity required to run the car (usually expressed in kilowatt-hours) in another unit of energy: gallons of gasoline" (para. 2).

While the future may hold developments such as inductive power transfer (IPT), electric cars, for now, are still limited by what their batteries can hold and concerns about where and how quickly they can charge. Oddly enough, inductive power transfer would essentially turn our highways into trolley tracks, like those developed in New York City to prevent damage to above ground cables and wires, supplying power from the road itself. The technology works by inducing magnetic current in a similar fashion to the new wireless charging pads marketed to make keeping devices charged simple and cord free: a technology featured in the Smart Home at the Chicago Museum of Science and Industry. A *Clean Technica* article on IPT discussed the vision of a New Zealand company, HaloIPT, that proposes that cars be fitted with a pad underneath the car which would pick up a charge from underneath the asphalt in a parking space or even along the highway: "roads already have an electricity infrastructure for street lighting etc; with an upgrade it could easily support the pads" (Milton, 2010, para. 9).

As the effort to informationalize the electric grid continues, the electric car presents a unique opportunity for electric utilities to utilize the power stored in car batteries as an alternative to bringing coal-fired peak power plants online when managing spikes in load. As infrastructure is informationalized in efforts to create a smart power grid, the possibilities for drawing on distributed storage by re-sourcing the power that drives individual mobility look more and more promising. Nick Chambers, the site director of *Gas 2.0* explains in a 2008 article that a plug-in hybrid vehicle that has extra energy stored in its reserve in the evening could sell that electricity back to the grid, and then charge in the early morning when electricity is less expensive, which would help to manage load at a potential profit to the consumer. After all, storing generated electricity is not only an issue of concern for electric

car manufacturers, but utilities as well. Managing load at an electric utility is a constant process of bringing power plants on and off line, and while some "storage" solutions exist—including banks of flywheels that store electricity as kinetic energy and the practice of pumping water uphill when there is extra energy so that they can produce energy by gravity when electricity is needed—distributed power storage has remained a challenge for utilities. Millions of batteries plugged into the grid and stored in garages at the drivers' expense present an opportunity for utilities to take advantage of distributed storage in ways never before possible. Though the electric car market is still developing, proposals for leveraging the distributed storage of electric cars as a grid management solution must be explored in terms of collective resource and individual mobility, particularly in terms of the car as service rather than the car as machine.

Social and Environmental Justice

To address an argument leveraged by oil companies to fight the deployment of public charging stations, I will next look to the argument that electric cars, while keeping downtown air clean, displace negative environmental effects to other (presumably poorer) areas. So, while downtown, exurban and suburban air would be increasingly free from petrol-based vehicle emissions such as carbon monoxide, formaldehyde, phenol, and acetaldehyde (which are some products of incomplete combustion in the internal power plants of cars), the deleterious effects of energy production would instead rise at power plants, located in rural and industrial areas so often ringed by low-income or poor workers and families.

While the Better Place video shows a white upper-class driver stopping by a windmill site (supposedly the driver is also a green energy worker), it is inconceivable that electric

vehicles will be powered exclusively by green or renewable energy sources in the near future. While dreams of electric cars powered by renewable energy play heavily in much of the marketing for these vehicles, the fact of the matter is that the energy that would power this mobility still comes from "unclean" sources. According to the U.S. Energy Information Administration (2011c) data on power generation by energy source, in 2010 coal-fired plants accounted for 44.9% of energy generation and petroleum-powered plants less than 1%. Importantly, burning fossil fuels creates a range of Hazardous Air Pollutants (HAPs). In an effort to better regulate emissions, the EPA initiated an Information Collection Request (ICR) on coal and diesel-fired electric generating utilities that asked facilities constructed after 1990 to test for their capture of a variety of HAPs, including those falling under the following categories: acid-gas HAP, dioxin/furan organic HAP, nondioxin/furan organic HAP, and mercury and other non-mercury metallic HAP (EPA 2009, p.1). Natural gas, generating approximately 23% of the total electricity in 2009, burns cleaner than coal and petrol products but is nonetheless a fossil fuel ultimately limited in supply.

In a 2010 *Scientific American* article titled "The Dirty Truth about Plug-In Hybrids," author Michael Moyer explains that "…during the time the car is on the road, it is truly a zero-emission machine. But at night, in your garage, that battery pack must refill the energy lost to the day's driving with fresh electrons culled from a nearby power plant. And zero emission it ain't" (para. 1). An accompanying multimedia presentation explains that the sources of power vary greatly depending on geographic regions, whether they are near hydroelectric, natural gas, nuclear or renewable resources. Moyer cites a North American Reliability Corporation report that claims that much of the energy that would power electric vehicles would come from coal and gas plants, as the hydroelectric and nuclear energy

sources are already spoken for through everyday use. While net carbon would be lower than petroleum-powered mobility in areas where power sourced from natural gas is available, in the Southeastern United States, where coal is a primary power source, carbon emissions would actually be higher as drivers converted to electric cars. The point is, "it's not just about what you're driving, but where you are driving it" (Moyer, 2010).

On the one hand, data show that, even when powered by traditional coal-fired plants, electric cars still use energy more efficiently than gasoline-powered vehicles, which positions the electric car, even when powered by coal-fired electricity, as a pollution solution. On the other hand, concentrating this pollution outside of urban areas and spaces of consumption potentially represents a toxic displacement whereby the negative consequences of consumption are moved away from the spaces of consumption. While the net benefits of centrally powered automobility are clear, with electric vehicles converting 75 percent of stored energy into power compared with 20 percent conversion of energy to power with internal combustion of gasoline (Greenemeier 2009, para. 6), the lived consequences of centrally powered vehicles on proximal communities may be hazardous. Without strict environmental regulation of power plants, the net environmental benefit of centrally powered mobility would suffer. Given lack of government support for EV initiatives in the early 2000s and demonstrated laxity in terms of energy and transportation sectors (clear in the move to cap and trade rather than raising standards), a clear regulatory framework that understands a major shift in energy consumption from distributed combustion to centralized generation is needed before large-scale moves to electric vehicles can be considered environmentally and socially just.

A second concern involves the relocation of waste. As with the removal of wastes to landfills and sewers (Huler, 2010, Marvin, 2010), the shipment of electronic waste to the developing world (Parks, 2004), and poignantly in cases of 'safely' disposing of spent nuclear cores, electric cars store energy in batteries which will need recycling and/or disposal. While the move to lithium-ion batteries represents gains in energy storage as well as reduced environmental impact, vigilance in recycling of battery materials are crucial, particularly as the packs rely on metals that could, like oil, become scarce.

Foreign Dependency

While the incorporation of electric vehicles into the automobility system could significantly reduce dependence on foreign oil, it would at the same time increase U.S. dependency on foreign metals. While lithium (the metal of choice for lightweight electronics and car batteries) is easily recycled, sources in the U.S. are limited. According to the *Latin Business Chronicle*, 70 percent of the world's salt lake lithium deposits are in Latin America (Colomar-Garcia & Zhao, 2011, para. 3). They explain that while there is a great potential for export markets to develop in many Latin American countries, in Bolivia, which is home to nearly half of the world's lithium deposits, production may be limited due to the country's political climate. Under the leadership of President Morales, the Bolivian government has created a state company in an effort to ensure that the nation's lithium deposits translate into wealth for Boliva, with operations from discovery to vehicle manufacture taking place within the country (Brown, 2010). Colomar-Garcia and Zhao (2011) explain that the prevalence of lithium in Latin America will attract outside investment from countries such as China which cannot mine lithium fast enough to meet demand. Infrastructure in the region is keeping

pace: “[t]he expansion of the Panama Canal, which will give rise to a class of supersized ‘New Panamax’ vessels, will further strengthen this demand in the region” (para. 12).

Ricardo Salvatore (2006) explains that the original construction of the Panama Canal served as a “spectacular machine” and “marked the ascent of the United States to a position of international leadership” in the larger effort on the part of the United States to position itself as a technological power in Pan-America (p. 664). While full control over the canal was in the hands of the Panamanian government in 1999, both the enlargement and a proposed alternative to the canal—the Chinese-Columbian transcontinental rail line— can be seen as continuations of elite and foreign power leveraging large scale infrastructure projects in order to gain increased military and financial control over the region. Wiley (2004) argues that one cannot understanding national space without “examining how it is connected to and dependent upon other contexts and broader regional and global flows” and cites the build out of U.S. rail and telegraph infrastructure as relying heavily on inexpensive copper and nitrates from Latin America (p. 84). In thinking about the move to electric automobility (both in China and the U.S.), we must consider the impacts of resource extraction more broadly: while many point to the Iraq War as being about oil, it is important to consider that part of U.S. presence in the region in general involves protecting power and sources of energy more broadly. Though lithium itself is not a source of energy, it is certainly the storage medium of choice at the moment, and so we must remember that decreasing our dependency on foreign oil by moving to the electric car will not make the U.S. independent of foreign resources.

The Promises

With both manufacturers and consumers interested in the electric car, the remaining challenges to widespread adoption of the electric alternative lie in access to and storage of power. Availability of electric car infrastructure and investment in further development and deployment of that infrastructure is crucial in providing a layer of "net-work" necessary between the electric grid and the driver. Tim Carey quotes R. James Woolsey, venture partner with a firm that invests in clean technology and former CIA director as saying: "What you're seeing is a divorce between the auto and the oil industries. Now, the utilities and auto industries will work together" (2010, p. 56). Given the longer history of utilities and transportation in the U.S., the move to the electric car can be seen as a logical return to an earlier system: when understood in terms of mobility thought large, the shift can be seen as both as a "divorce" from gasoline and a reconciliation with electric utilities.

This return comes at a time when utilities are seeking new ways to sell power (dynamic pricing) and invest in infrastructure (smart meters, information architecture), the electric car presents not only a site for the consumption of power, but also a resource for managing load as utilities look to invest in less consistent clean energy solutions (such as solar power, which is only available during daylight hours in clear weather conditions; and wind power, which generally blows strongest at night when fewer people are using electricity). With millions of batteries offering a place for that power to go in the wee hours of the morning, while at the same time serving as a potential source of power on a rainy day, utilities are interested in more than selling power: they are interested in leveraging electric mobility to manage it. The potential for the electric car to serve the needs of a larger private entity demands further exploration.

Dennis and Urry (2009) and many post-peak oil activists explain that the present automobility system is unsustainable: constructed based on a substantially lower fuel-cost to income ratio and locked-in due to scale and cost of development, the system becomes increasingly expensive to use and maintain as fuel is more difficult (and expensive) to extract. While the present automobility system was built with fossil fuels for fossil fuels, electric automobility can build infrastructures with fossil fuels for clean energy. In the short term, electric automobility will be powered by energy from coal, but because the car does not have to process the energy source directly, nothing will change for the user when clean alternatives are available—no adapters, no kits, no adjustments— the electricity coming down the wire will just come from somewhere else. As new clean energy sources are utilized, the infrastructure will serve them. Cars may not run on sunshine, but they might run on electricity coming from a solar plant or home solar panel that runs on sunshine. In moving automobility to a nexus system that drives like a series system, the EV industry promises American drivers that they can continue to live in the suburbs, come and go as they please, and sit in traffic just like always with the benefit that it will also be affordable, environmentally conscious, and communication rich.

A Smarter Grid, A Smarter Car

Informationalization is the central component that will drive electric mobility, and this same process is occurring in a number of related infrastructures and in automobility more broadly as automobiles are becoming less machines that a driver operates and more centers of communication in which an operator moves. From OnStar to Ford Sync, the automobile is marketed more and more as a comfortable space in which users can be mobile while

communicating, with Nissan taking things a step further by calling their Cube a "mobile device" (Nissan, 2011). In addition to music (which has long held an important place in the automobile), the adoption of mobile CB radio later enabled drivers to maintain a connection with other drivers as later with the home and office (fixed points) before finally connecting with the larger telephone network via the car phone and later the cellular phone (Packer, 2002; Packer and Oswald, 2010). The early 2000s saw the adoption of navigation devices using the Global Positioning System (GPS), and in more recent years, the Internet. Automobile and communication networks are being further integrated through the use of on-board platforms such as OnStar, Ford Sync, Chevrolet MyLink, and the move to "carputers" that enable the car to become accessible via networks in new ways.

The car as a mobile device begs the question of what the role of "smart" is in an increasingly connected automobility system. Examining the relation between automobility, safety, and security, Packer explains in *Mobility Without Mayhem* (2007) that many C3 (communication, command and control) technologies "such as the global positioning system (GPS), onboard computers, and integrated surveillance cameras, are publicized as upscale commercial goods whose only values are those of personal convenience, safety, and freedom" (p. 25). Next, I look to one such example in an advertisement for the Buick Lacrosse in which control at a distance becomes a salient consumer perk.

In a recent commercial for the Buick LaCrosse, General Motors features a new Buick mobile application. The primary driver's daughter and her friend stand in a driveway outside of a large home next to a 2011 Buick Lacrosse, and daughter calls dad to ask if she can borrow the car:

Daughter: So How's London?

Dad: Oh, it's amazing.

Daughter: Dad, can I use the car?

Dad: Uh, let me check…

Voiceover: Introducing Buicks' new mobile app. It lets you check and control your Lacrosse from your right smartphone. From almost anywhere.

[Dad scrolls through an app that shows on one screen with options to lock, unlock, start, and cancel start before moving to another screen showing fuel available, trip, and fuel efficiency; and a third screen that shows the pressure in each tire]

Dad: OK, but promise to have it back by 10.

Daughter: Thanks Dad!

Dad: OK, I'll start it up for you (starts the car remotely from the application)

Daughter: (hanging up) Oh, come on

Friend: Seriously (Buick, 2011)

This application is yet another indication of the informationalization of transportation, and further demonstrates that the smart car is not necessarily an electric one. The application not only serves the role of extending telematics beyond the dashboard, but in fact brings the car a step closer to being a remote controlled car. If it is possible to start the car from a distance, when will the driver have the capability of stopping the car from a distance at the push of a button (as OnStar already does)? As smart features such as park assist, lane assist, and advanced cruise control are incorporated into the automobile, it seems more a question of when than if applications will enable a driver to "call" the car to the curbside from a smart garage in which a valet will never have to hold your keys. The car might even tip him for lifting the gate for you on the way out.

A smarter planet requires, according to IBM, a process of instrumenting, interconnecting and making systems intelligent, and the car is poised to undergo a shift in the United States that will move it closer to this goal. The Cameron Gulbransen Kids Transportation Safety Act of 2007, signed into law in 2008, directs the U.S. Department of Transportation to propose safety regulations to prevent death and injury caused by backup accidents, which the National Highway Traffic Safety Administration estimates lead to 292 fatalities and 18,000 injuries per year (NSTSA, 2010). While the NHTSA has asked for a delay in proposing final regulation, the plan (as it stands) would require backup cameras in all new vehicles by 2014 (Healy, 2011). Mandatory backup cameras represent a real step in a process of informationalizing automobility: one more required instrument in the car that, while effective in reducing backup crash deaths and fatalities, would also put the vehicle one step closer to capabilities such as park assist, lane assist, and automatic cruise control that require similar hardware and software.

As safety is used to legitimate the regulated inclusion of hardware and software that will make the car smart, it is imperative to look to security concerns in the car. A 2010 study by a team of researchers titled "Experimental Security Analysis of a Modern Automobile" explored a number of potential attack vectors in automobiles, from Bluetooth networks to iPods, demonstrating the potential for cars to be interfered with or controlled remotely (Kosher et al). Based on experiments in both lab and track environments, researchers found that systems in cars, while often made safe from failure, were not secure from attack (Kosher, et al, 2010). As the car increasingly is prepared for informationalization through the inclusion of both mandatory and optional smart features, the network security of the car may well come to rival concerns about its physical safety.

The next chapter looks at net-work security more largely, turning to focus on the potentials for cyberwar that became actualities after the successful cyberattack on Iran in 2010 delivered via the Stuxnet worm. After reviewing media coverage of the attack, I look to U.S. cybersecurity and critical infrastructure protection, focusing on the role of the public-private partnership in making cyber attack and critical infrastructure protection a reality.

Chapter 3: Critical Infrastructure and Smart War

While infrastructure convergence has enabled a variety of conveniences from electric cars to smart grids, it also presents new vulnerabilities brought on by increased simultaneous dependence on multiple shared infrastructures. As users increasingly take interconnected networks as given, understanding the ways in which mobility and consumption play out across multiple systems at once – at a nexus of nexus systems – is increasingly central to the management of life in informational society. Unless multiple redundancies are integrated into platforms, the failure of any one component has the potential to cause decreased performance or failure of the entire platform. In the case of the electric car, failure in electric generation, transmission, or distribution; failure of the battery, an issue with the payment system at the plug, or a failure in the network within the car or its mechanical components can mean immobility. Networked practices are supported by overlapping webs of infrastructure and systems, and ensuring that all of the necessary components do not fail is critical to the smooth operation of daily networked life.

In "Postscript on control societies," Deleuze (1997) explains that unlike disciplinary society where "man provided energy in discrete amounts," in control society man "undulates, moving among a continuous range of different orbits" (p. 180). Moving through these orbits necessitates the negotiation of increasingly complex assemblages of infrastructure, resources, and protocols through flexible and dynamic control. While disciplinary man *used* infrastructure, control man relies on its *modulation* to go with the flow, using a range of convenient (fitting) technologies that translate energy, data, and services into something that can be turned on, used, and turned off. Informationalization makes this negotiation possible.

Not only convenience, but also necessity drives the use of multiple infrastructures simultaneously: as informationalization drives new interdependencies in energy, transportation, and communication, it is not only convenient but also increasingly necessary to use multiple infrastructures at once. Without energy, either from a steady flow available at the wall or packetized units (batteries), we find that our appliances and devices will not work. Without connected communication infrastructure, credit card purchases are a cumbersome analog process of taking a rubbing of a card on a crude device with the assistance of carbon paper. When power is disrupted in transportation, the intersection is called into question as a space of movement, and (if we are lucky enough to be driving on a well-travelled road) an officer of the law will work to restore order to ensure it is only roads and not automobiles that intersect. Simultaneous reliance on multiple infrastructures is not only what makes life in networked society convenient, but also possible, and concerns for vigilance, resiliency and rapid restoration in the face of failure and attack are a major focus of the corporations, governments, and militaries around the world that are ultimately responsible for building, maintaining, and securing those Deluezian "orbits."

With recent developments proving that cyber threat is actionable, nations around the world work on the one hand to secure critical infrastructure (CI) while developing "cyber capabilities" on the other. This chapter explores critical infrastructure in terms of failure and attack through an examination of both the changing definition of critical infrastructure and new practices of war. The changing definition of what constitutes critical infrastructure indicates increased concern about attack over concern about failure (indicating a shift in focus from safety to security) and needs to be examined in the context of increased efforts to secure the foundations of America as an operational nation state from unknown threats.

While these threats are increasingly uncertain and unknown, the changing strategies and tactics of the U.S. military offer some insight into the nature of them. Through an examination of the revolution in military affairs currently taking place in the U.S. and abroad, I hope to reconcile increased attention on securing infrastructure with the newly developing strategies and tactics that warrant such measures.

Many ways of talking about changing notions of war that have emerged in the second half of the 20th century including infrastructure war, netwar, information war, cyberwar, cyberterrorism, and operations other than war and have animated scenarios such as the "Electronic Pearl Harbor" discussed by John Carlin in his article "Farewell to Arms" (which later became the core of the plot of *Live Free or Die Hard (2007),* only re-named "fire sale"). As far back as *Wargames* (1983) the American public began to imagine the damage that a hacker could do when interfering with a military system – what we would consider today to be cyberterrorism. Arquilla and Ronfeldt's (1996) argument that "it takes networks to fight networks" speaks to reorganizations in strategies to protect the homeland, but also new strategies leveraged in war and operations other than war to "secure" resources and strategic footing in the homeland of others (p. 82). This chapter analyzes strategies of targeting dual-use infrastructure through both traditional and cyber ordnance.

I begin by examining the relation between infrastructure and war by looking to the origins of the term "infrastructure" in the United States as it relates to the military concepts of strategic mobility and logistics as well as post-WWII rebuilding in Europe. I then discuss infrastructure war broadly through the work of Stephen Graham before addressing a shift in delivery method from bombs to bits in targeting infrastructure. As military tactics leverage command, control, communications, computers, combat systems and intelligence (C5i)

technologies in increasingly central roles in order to turn the infrastructure against the system, I use the deployment of the Stuxnet worm that targeted nuclear enrichment facilities in Iran in 2010 as a case to illustrate a shift in thinking about infrastructure war and examine what such a shift means for both operations abroad and vulnerabilities at home. I argue that thinking of the worm in terms of cyber ordnance goes a long way towards clarifying what are often ambiguities about the role of information weapons in a new kind of war.

After discussing the development of new strategies of warfare and of peacekeeping that accomplish target compliance through the manipulation and destruction of dual-use infrastructures (those that are used for both military and civilian purposes), I examine the development of the notion of "critical infrastructure" (and efforts to secure it) in the United States. Originally referring to the adequacy of public works, the term has since come to encompass expansive strategies of protecting the homeland by securing her infrastructure. Having established the legitimacy of the cyber threat, the remainder of this chapter reviews a history of critical infrastructure protection and cybersecurity efforts both before and after 9/11, situating cyber ordnance as part of a larger program of infrastructure defense (and war).

Infrastructure and War

According to Lewis (2008), infrastructure is a French loan word that originally referred to railroad engineering and was quickly situated within a military context when it was later used within NATO to refer to the necessary installations to secure post-WWII Europe (para. 11). The Oxford English Dictionary cites the first English language use of the term in *Chambers's Journal* in May of 1927 ("infrastructure") to refer to rail line construction and later in the 1950s to refer to military installations. This was certainly the

case with the founding of NATO's Infrastructure Program which pooled the money of member countries in order to build shared infrastructure in post-WWII Europe. One of the ways in which "infrastructure" came to be understood was through shared investment in fixed military installations that would later protect and work to establish secure paths of global trade (Deborah Cowen explains that the term "logistics" shares a similar origin). In many ways, then, war is the genesis of our notion of infrastructure, and though war is not the driving factor in all infrastructure development, programs since World War II have worked to articulate infrastructure in particular ways for purposes of both strategic mobility and, later, homeland and global security. As will be discussed in this chapter, communication infrastructure, particularly in its role in informationalizing a range of other infrastructures, is perhaps the most critical infrastructure sector of the many identified by the U.S. Department of Homeland Security.

In his article "Sublimity and solutions: Problematization in ICT for development perspectives" (2008), Chris Russill problematizes global information communication technology (ICT) development, suggesting that while ICT development is often framed in terms of a digital sublime, when demystified, it becomes apparent that rather than working to advance underdeveloped countries, ICT rather works to capture them in neoliberal governance. While the focus of this dissertation will not be on processes of infrastructuring and ICT deployment, literatures describing their development are essential to understanding the processes of globalization and uneven development that enable the continued expansion of capital and military dominance. What I examine here is more specifically the processes by which these investments come to be securitized (in both military and economic senses of the term) in a broad way through policies, partnerships, and military doctrine.

In this same trajectory, Graham and Marvin (2001) examine cities from 1850-1960, identifying this time period as one where a focus on infrastructure became a concern among city planners and mass and industrial scaling began to facilitate increased exchange "through widening nets of superimposed and interconnecting pipes, tracks, roads, wires and conduits" (p. 40). Such expansion tracked parallel to the emergence of a mass culture that expanded further after the Second World War, mass-production, standardization, and urban planning. Graham and Marvin position urban planning in this period as part of a larger project of modernization that would rationalize the space of the city though technology, which they explain was initially understood in terms of views of the city as an engineered system and later as part of a broader technological (and later electrical) sublime. Taken together, we can understand infrastructure as being tied with mass culture and mass production, nation building, post-WWII nation rebuilding, and urban planning: as the establishment of a grid thought large on which social, economic, governmental and global activities can be carried out, managed and manipulated. Infrastructure is critical to governance, national and international commerce, public health and safety, military operations and global as well as homeland security, making it essential for modern life and participation in the larger global economy. "Criticality" also makes it a primary target in terrorism and war.

Infrastructure Warfare

While, in the U.S., critical infrastructure (CI) was long thought to refer mainly to the safety of public works, developments in military and terror tactics at home have forced planners to consider infrastructure as a potential target much more broadly. The changing definition of CI over the past 20 years reflects a change in focus from the safety of essential

infrastructures that we are told are in disrepair and decay to securing those infrastructures from attack. The impetus behind such efforts to "secure" rather than "make safe" are in many ways a response to a new strategy of warfare embraced by the U.S. Military that targets enemy societies rather than enemy combatants in order to achieve desired effects.

Steven Graham's work on infrastructure and military urbanism considers infrastructure through the lens of warfare, including an examination of tactics targeting "dual-use" infrastructures. To elaborate, dual-use infrastructures are seen first as permanent or semi-permanent military installations, designed for the efficient and rational movement of people and goods (soldiers and supplies), information (communication), and energy (rations and power); and in the second, as personal and commercial infrastructures for moving goods and people (commerce, commuting and leisure), information (communication, media), and essential services (water, gas, electric, sewage, etc). More than simply a foundation for military action, these infrastructures are tied up with other infrastructures essential to life itself, and are therefore a particularly important site of analysis. Graham (2005) explains that urban infrastructural warfare aims for "organized, systematic de-modernization not just of the military forces of those deemed to be enemies, but of their urban civil societies as well" (p. 178). "Systematic de-modernization" is accomplished through the generation of second-order effects including the contamination of drinking water and disruption of communication and transportation that lead to third-order effects including limited food supply, increased rate of disease, and the disruption of civilian communications.

Graham (2005) cites specifically the 1999 military operation in Kosovo ("systematic de-electrification") and the Iraq wars in 1991 and 2004 ("the war on public health") as cases where U.S. Military tactics of precision-based non-lethal destruction using weapons such as

electromagnetic pulses (EMPs) and carbon bombs (designed to disable electronic equipment and switches) had severe negative effects on the civilian population. In these cases, the destruction of dual-use infrastructures ultimately brought about second- and third-order effects such the failure and contamination of water supplies that lead to widespread disease: effects not considered attacks directly on civilian population, but instead adverse effects stemming from the strategic targeting of dual-use infrastructures. Further, Graham notes, as infrastructures are increasingly linked with communication systems, strategies to engage in and defend against computer network attack (CNA), or "deliberately manipulating computer systems to disable an opponent's civilian infrastructure" are being researched and developed in the U.S., and were even discussed as an option on the war on Iraq (2005, p. 186). These tactics, he argues, are part of a larger shift in focus that moves away from the destruction of infrastructure and instead toward concerted efforts to control it remotely, further distancing the actor from the effect and in many cases leaving the infrastructure largely intact.

The manipulation of infrastructure, Graham argues, plays an increasingly important role in geopolitical struggles and complicates the ability to discern where war begins and ends in space and in time, much in the vein of Virilio's suggestion that *total war* has come to describe moves to an increasingly militarized everyday life. Another key issue arising from the prevalence of these strategies is an inherent "militarization of all the aspects of contemporary urban societies" such as a perceived state of perpetual danger that leads to increased securitization, surveillance and control (Graham, 2005, p. 189). Graham (2005) argues that while efforts to make infrastructures more resilient against disruption are important to defense, "reorganizing cities and their infrastructures based on notions of near-absolute security would quickly have such devastating consequences on the very interactions

and flows that enable urban life to thrive in the first place that cities would soon become untenable" (p. 190). Graham cites a disconnect between studies in political violence and urban studies as part of the lack of knowledge about the vulnerability of cities and infrastructures, and that this area needs to be explored so that the impacts and threats that these strategies pose are neither under- or overestimated. He argues that further obscuring the importance of this topic is the media focus on immediate casualties associated with war and a neglect of broader infrastructural impacts, and calls for "a sustained and interdisciplinary engagement with the multi-scaled geopolitics of everyday technics and urban infrastructure" (Graham, 2005, p. 190).

While the reorganization of infrastructure in terms of absolute security makes the orbits of the contemporary city less navigable, without a certain level of circumscription, the city (and nation) loses its ability to hold territory and effectively direct and redirect flows. In this sense, we can imagine infrastructure as having an important function in holding territory—personal, commercial, and military—through the management of flows. When infrastructure is targeted, second- and third-order effects (such as loss of critical infrastructure in the civilian population including electricity and water and the subsequent lack of faith in leadership) deterritorialize space: in cutting the sinew that holds territories together, spaces are undone and become subject to new arrangements. As infrastructure warfare moves to cyber mediation, *manipulation* rather than *destruction* of infrastructure plays an increasingly important role, and informationalized infrastructure will vastly expand the ability to "scan" the earth, which Virilio argues is central in the ability to hold territory (1975/1994).

Cyberwar

Efforts to secure critical infrastructure and key resources go beyond direct physical attack on critical infrastructure. Despite best efforts to secure critical infrastructures and key assets such as nuclear facilities, ports (see Cowen, 2009, on DESA certification and port cities), and perhaps most visibly those of air transportation (the establishment of the TSA and an ever-evolving program of airport security measures), securing infrastructure and maintaining its usability increasingly demands the development of programs that leverage informationalized infrastructure to secure transportation (camera based speed limit enforcement) data traffic (packet sniffing) and utilities (the smart grid). As informationalization continues to facilitate the efficient and safe operation of transportation, utility, public health and military infrastructures, information networks present themselves not only as a means of enabling efficient operation, but also a high-value target and a vector of attack. The net-work of dependencies that affords next-generation smart grid services, smart transportation, and telemedicine are the same links that most threaten the continued access to utility services, mobility, and access to emergency services, as they serve as a vector for cyber-attack.

The potential for network-based attack is not new, though a number of current efforts suggest that newly increased attention is being paid to securing critical infrastructure. Challenges associated with these efforts deal with the uncertainty of the origin of cyber-attack, further complicated by the incorporation of mobile technologies and wireless and mesh networks that make tracing the origin of an attack increasingly challenging (if not impossible). There are also a number of political challenges associated with cybersecurity, including poor coordination between the public and private sector in efforts to assess risk,

ambiguities as the law works to catch up with technology, and a lack of centralization in cybersecurity efforts which are presently distributed among a range of departments, agencies, and offices with different approaches and perspectives (Theohary and Rollins, 2009).

In a Congressional Research Service report for Congress, Theohary and Rollins (2009) define "cybersecurity" broadly as "the protection of critical information infrastructure and its processes and content" (p. 2). The report provides an overview of current executive branch initiatives concerning cybersecurity, including the Comprehensive National Cybersecurity Initiative (CNCI), the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, and the White House 60-Day Cyberspace Policy Review. The 2008 CNCI, brought into being through two classified presidential directives (DHS Presidential Directive 23 and National Security Presidential Directive 54) focuses on tactical plans for securing CI while the creation of the CSIS Commission on Cybersecurity calls for a national cybersecurity strategy and regulation of cyberspace, as well as the reinvention of the public-private partnership (PPP). I will discuss the most recent effort—the White House 60-Day Cyberspace Policy Review— in more detail, as it outlines a new approach to securing cyberinfrastructure, particularly in terms of the transparency of its objectives.

In a May 2009 White House Office of the Press Secretary "Remarks by the President on Securing our Nation's Cyber Infrastructure," press release, Barack Obama explains the benefits and dangers of increasingly connected information networks, situating cybersecurity as key to economic prosperity, national security, and American Military prowess. "In today's world," says the Oresident, "acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer – a weapon of mass disruption"

(para. 15). The use of "disruption" rather than "destruction" can be seen here as more than rhetorical flourish, and in fact it points to a much more significant shift in the ways that terrorism is thought of in terms of information networks.

Immediately following this, Obama mentions an attack on military networks that led to the military moving away from the use of USB memory sticks (a.k.a. thumb drives or flash drives); USB drives had been used as an attack vector to spread malicious software, or "malware" into control units at the Nantz nuclear enrichment facility in Iran and the Russia-Georgia conflict in which Russia carried out a cyberattack on Georgian government networks in order to compliment traditional warfare tactics (2009). Further discussing the piecemeal nature of cybersecurity efforts, Obama explains that after taking office, he began to conduct a review of federal efforts to secure information networks through the 60-Day Cyberspace Policy Review, which is to be the foundation for a new approach to national cybersecurity. The new approach takes cyberinfastructure as a key national asset, calls for the appointment of a Cyber Czar, and focuses on five main areas: 1) developing a comprehensive strategy; 2) organized and coordinated response; 3) strengthening the public-private partnership; 4) a renewed focus on research and development; and 5) digital literacy. Above all, the statement announcing the report stresses a continued respect for a free and open internet as well as private internet traffic. (It should be noted here that Obama says nothing about Stuxnet, the worm that targeted Iranian nuclear facilities in 2010.)

Next, I look to the possibilities for further U.S. Military and legislative crackdown based on recent events that proved, for the first time, that cyber threats are legitimate. I examine the media coverage and ramifications of the first successful cyberattack on material infrastructure—the Stuxnet worm—which, rather than aiming to disrupt information

networks, targeted the software controlling specific articulations of mechanical equipment with the end goal of material effects. I will examine the discursive and structural impacts of Stuxnet, ultimately arguing that the worm will serve as a lynchpin in future arguments concerning cyber and infrastructure security. I then configure Stuxnet as signaling a new chapter in the history of mediated warfare now that once-theoretical cyberweapons have become embodied in practice, examining what makes Stuxnet different from other forms of information war, suggesting that cyber ordnance (digitally mediated artillery) plays a critical role in a new kind of smart war.

Stuxnet: Infrastructure Warfare goes Online

> I am afraid this is the beginning of a new world. 90-ies were a decade of cyber-vandals, 2000's were a decade of cybercriminals, I am afraid now it is a new era of cyber-wars and cyber-terrorism. (Eugene Kaspersky, quoted in Kaspersky Labs 2010 para. 8)

In June 2010, a Belgium-based security firm, VirusBlokAda, discovered Stuxnet, the first known computer worm that attacks Supervisory Control and Data Acquisition (SCADA) systems in an effort to target critical infrastructure (Beaumont, 2010). *Wired* writer Kim Zetter explains that the worm works specifically by targeting high-priority data blocks in SCADA systems used for critical and high-pressure situations and, once installed, cloaks itself by displaying what amounts to an image of the previous software while disabling security mechanisms. The vector for the worm is believed to be USB memory sticks (discussed in Obama's 2009 statement), which offer storage of large amounts of data in a light-weight and highly mobile form. USB portability enables the worm to enter even seemingly closed networks by moving on physical hardware carried by persons rather than external networks. In September 2010, security experts were divided on whether or not the

attack had already occurred or had yet to occur, whether the Middle East was the target, possibly Iran, or more specifically nuclear facilities in Iran. There was also disagreement early on as to the purpose of the worm (attack, espionage, or both) and whether or not the effort was necessarily state sponsored. As more facts became available, experts speculated the specific target of the attack to be Iran's Bushehr nuclear power plant. Others pointed to evidence that the target was an enrichment facility in Nantz, citing a 2009 WikiLeaks report of an accident at the facility and data from the Federation of American Scientists (Zetter, 2010). Zetter claims that this data corroborates the hypothesis that Iran was a target and "show[s] that the number of enriched centrifuges operational in Iran mysteriously declined from about 4,700 to about 3,900 beginning around the time the nuclear incident WikiLeaks mentioned would have occurred" (2010, para. 25). This timeline suggests that Stuxnet was likely operational a year before its discovery by VirusBlokAda.

In a statement on their website, computer security firm Kaspersky Lab explains that while there was not enough evidence to locate the source of the attack – a common challenge to most cyber threats—they "can confirm that this is a one-of-a-kind, sophisticated malware attack backed by a well-funded, highly skilled attack team with intimate knowledge of SCADA technology" that they believe "could only be conducted with nation-state support and backing" (2010, para. 2-3). The worm takes advantage of four "zero-day exploits," best understood as vulnerabilities tergetted before software developers and security companies can close the hole or patch the vulnerability (Contos, 2007). Kaspersky Lab explains that an analysis of the code by their security experts indicates that the goal of the worm was both to gather intelligence and to sabotage the system, and that the targeted nature of the attack, the complexity of the code, and the combined intelligence-gathering and sabotage elements of

the worm point to the presence of a nation state behind the development of the worm: "Stuxnet is a working – and fearsome – prototype of a cyber-weapon, that will lead to the creation of a new arms race in the world. This time it will be a cyber-arms race" (para. 13). It is generally agreed upon that the Stuxnet worm marks "a shift away from malware deployed for financial gain to controlling critical machinery" as part of a "third age" of cybercrime (Halliday, 2010, para. 20). Network security company Sophos' 2010 *Security threat report* explains that while hacking was once largely a hobby that became an organized criminal activity, "[a]s we enter 2010, it can be argued that there is more evidence than ever before that a third motivation is driving cybercrime: using malware and the internet to gain commercial, political, economic and military advantage over rivals" (p. 34).

As is often the case in the reporting of technical matters in the popular press, reports of Stuxnet have been rife with inaccuracies that complicate an already complex issue. For instance, an article in *The Telegraph* from 2010 inaccurately identifies the act as "cyber terrorism, a virus written and sanctioned by one country with the aim of impacting the infrastructure of another" (Beaumont, 2010, para. 1). This statement contains a number of inaccurate points, and is one example of a tendency in the popular press to not only use terms that some consider very technically specific interchangeably (Stuxnet was a worm rather than a virus), but to conflate cyberterror and cyberwar. As distinctions between war and operations other than war as well as the numerous wars on concepts such as terror, poverty, and drugs continue to blur the definition of "war," the differences between cybercrime, cyberterror, state-sponsored cyberterror, and cyberwar will be vital in terms of understanding such attacks.

Many reports indicated that an attack of this complexity could only be carried out with the resources of a national intelligence service or a nation-state, and with publicly disclosed funding of such efforts, the United States and Israel have been identified as likely points of origin. In a news story on the worm, Reuters security correspondent William Maclean cited comments made to the press by Sean McGurk, who runs the National Cybersecurity and Communications Integration Center, as explaining that identifying the origin of the worm was not the first priority of the center, with immediate efforts instead focused on the mitigation of the effects of the worm as well as efforts to prevent the spread of the code which targets "programmable logic controllers" that operate physical machinery (2010, para. 9).

At present, Stuxnet is no longer a threat. According to an article in *PC World*, computer security company "Symantec gained control of the domain used to send commands to infected machines shortly after Stuxnet was discovered, meaning that the hackers behind it no longer have a way to send new commands to infected systems" (McMillan, 2010, para. 15). It is interesting to note here that control of the situation has been credited to a private company and not the U.S. military or government, further evidence to suggest the extent to which public-private cooperation is relied upon in cybersecurity efforts. As experts reverse engineered the code, they discovered that the worm was able to monitor settings and then potentially take control of the systems mentioned previously, and after further research many experts are confirming that "Stuxnet is essentially a precision, military-grade cyber missile" (Clayton, 2010, para. 11). Much news coverage in September 2010 focused on the weapon-potential of this worm, perhaps the first prominent example of a future line of information weapons. German cybersecurity expert Ralph Langer has dissected portions of the worm

code on his website, and through his analysis he observed that a step that he terms "fingerprinting" gives the worm targeting potential, as it seeks specific articulations of hardware and software in supervisory control and data acquisition (SCADA) systems. Clayton of the *Christian Science Monitor* writes: "For those worried about a future cyber attack that takes control of critical computerized infrastructure – in a nuclear power plant, for instance – Stuxnet is a big, loud warning shot across the bow, especially for the utility industry and government overseers of the US power grid" (2010, para. 25).

To be clear, many are claiming that the Stuxnet worm could make Iran the first "real" victim of cyberwarfare. In a September 2010 *New York Times* article, John Markoff claims that "security specialists who have examined it were almost certain it had been created by a government and is a prime example of clandestine digital warfare" (para. 4). A main point of concern in the article is the question of why the creators of the worm would allow it to spread so widely: did a government push for the launch of the worm before it was ready in order to stop enrichment in Iran? Is this actually the first such attack? Markoff (2010) argues that while Stuxnet has drawn much media attention, "it is likely that there have been many other attacks of similar or even greater sophistication by intelligence agencies from many countries in the past. What sets this one apart is that it became highly visible" (para. 17), citing the 2005 discovery of a Trojan horse infiltration of a Greek cellphone network and questions surrounding a 2007 Israeli attack on Syria where a "kill-switch" shut down Syrian radar systems, but culprits were never clearly identified.

Again, with Stuxnet, all signs point to the U.S. and Israel. In January 2011, the *New York Times* journalists William Broad, John Markoff and David Sanger presented evidence that suggests that the worm was tested at the Dimona complex in Israel, which is also said to

be the site of the country's nuclear weapons program. With U.S. and Israeli officials speculating that Iran is no longer "on the cusp" of developing nuclear weapons, the journalists speculate that "The biggest single factor in putting time on the nuclear clock appears to be Stuxnet, the most sophisticated cyberweapon ever deployed" (para. 8). While the origins of the worm are yet to be identified and officials in both the U.S. and Israel have not taken credit for its effects, the article points to evidence that suggests U.S. and Israeli involvement "with some help, knowing or unknowing, from the Germans and the British" including cooperation between the Siemens Corporation and the Idaho National Laboratory in 2008 regarding assessing vulnerabilities in control systems (para. 19). The report cites a conference paper and presentation at the 2008 Automation Summit conference by Marty Edwards of the Idaho National Laboratory and Todd Stauffer of Siemens as openly demonstrating vulnerabilities of control systems used in many industrial applications in the U.S. and around the world, including the facility in Nantz. These devices became a subject of interest in relation to Iranian facilities, which is further shown through cables made available on WikiLeaks that point to sanctions efforts around Siemens controllers bound for Iran. The journalists also claim that the U.S. and Israel have facilities with P-1 centrifuges—those of the same design as those A. Q. Khan brought to Pakistan from the Netherlands in the 1970s and that are also currently being used in Iran— that are assumed to be used in Israel for enrichment for their own nuclear arms program and in both Israel and the U.S. as a testing facility to explore vulnerabilities. Media coverage fueled speculation of U.S. and Israeli involvement despite a lack of Iranian confirmation that a target had even been affected.

The targeting of Iran was confirmed in November 2010 when President Mahmoud Ahmadinejad reported that an attack had affected some of the countries' centrifuges and

delayed nuclear goals, though he minimized the effects of the attack publicly, calling it only a minor setback. One reported solution to the widespread infection (some reports indicate that approximately 30,000 Iranian computers are infected by the worm) involves the costly proposition of replacing systems and buying new centrifuges (Sanger, 2010; Warrick, 2011). There have also been calls for retaliation by Iran, with Iranian cybercrime outfits looking to create damaging worms and viruses as retribution for Stuxnet (McConnell, 2011).

Stuxnet has been called a "powerful weapon in the new age of global information warfare" and "a prime example of clandestine digital warfare" that may shape a new global arms race that is highly dependent on public-private cooperation in terms of defense and offense (Falkenrath, 2011, para. 1; Markoff, 2010, para. 4). Falkenrath of *the New York Times* asks us to imagine a future where companies align with government to support homeland security in the realm of cyberthreats (and therefore also cyberwarfare) or, in not complying, support consumer protection or foreign states. Further complicating the conveyance of cyberwarfare, he points out, is an absent international legal framework: "An international entity that could legislate or enforce an information warfare armistice does not exist, and is not really conceivable" and is complicated by issues "of private property, personal privacy and commercial integrity" (2011, para. 10; 13). The cooperation between Idaho National Laboratories and Siemens is only one example of this: more broadly, military and government networks are often indistinguishable from commercial telecom networks, complicating issues of who is responsible for defending and securing these infrastructures.

Warfare has been largely understood as acts of violence by one nation state on another, with non-state attacks generally framed in terms of terrorism or revolution. The distinction is valuable in discussing cyber conflict as well. Unlike an act of cybercrime,

cyberwarfare is the intentional attack of the network of one nation by another nation or group of nations. Speculation that the United States and Israel are behind Stuxnet would mean that the worm represents cyberwarfare rather than cyberterror or crime. Iran certainly feels this way: A BBC report cites a comment made by head of the Iranian IT Council at the Ministry of Industries, Mahmoud Liayi, in the state-run Iran Daily newspaper as claiming that "[a]n electronic war has been launched against Iran." Informationalization is a process occurring globally in a variety of processes for a range of purposes, and when platforms are used across systems and nations, the barriers to entry into those systems are weakened. Cyber approaches are less physical in their implementation than traditional approaches, and while effects (for now) may not be as immediate, they have the advantage of stealth. If the traditional approach (air strikes) equate to shooting an enemy with a machine gun, Stuxnet (which threw off the timing of centrifuges by a fraction of a second) is a little arsenic in the morning coffee for weeks. In this new conception of war, the battlefield is everywhere a network exists, the target can be anything of value, and the weapons have come to include cyber ordnance.

Cyber Ordnance

Computer security specialist Ralph Langer refers to the worm as a “dual-warhead” designed to both cause equipment to fail and to disable safety systems in an effort to cause an entire plant to self-destruct. Based on his analysis, “Stuxnet is not about sending a message or proving a concept… It is about destroying its targets with utmost determination in military style” (Langer, quoted in Broad et al., 2011, para. 44). With “fingerprinting,” the worm becomes a way to rearticulate force at specific points, to control enemy territory remotely, a weapon that can be targeted strategically like a smart bomb but without the material presence

of threat. Instead of introducing new material into the target site, it works through code to rearticulate infrastructure in destructive ways, taking up the infrastructure at hand and reorienting it toward destructive ends.

In a 2001 paper titled "Information War Crimes: Mitnick Meets Milosevic," Major Darwyn O. Banks of the United States Air Force at the Air Command and Staff College at Air University examines the area between information and war crimes. Examining potential adaptations of terms central in courts considering traditional war crimes in the Information Age, Banks explains that the international law of war is outlined in two sets of treaties—the Hague Convention focusing on "the means and methods of warfare" and the Geneva Convention which "deals more specifically with the status of non-belligerents and other protected persons"— that together can be described through four main principles: chivalry, humanity, military necessity and proportionality (p. 7-8).

Explaining that the "Martens Clause" of the Hague Convention in 1899 was designed to take changing technologies of warfare into account, Banks (2001) points out that law is continually, though not consistently, updated: for instance, while projectiles were prohibited from balloons, law was not updated to reflect this same prohibition in powered flight. Interested in the ways in which law will be updated to address information warfare, Banks explores both first-generation information war, which focuses on destruction of targets and second-generation information war which focuses instead on the information itself, aiming to attack enemy strategy rather than material targets. He argues that the former and not the latter will likely be the main focus in incidents violating international war law.

With Stuxnet, the lines between first and second generation information war are blurred. While the object of the worm is believed to *target* a specific location for destruction,

the objective was at the same time to attack the *strategy* of Iran – specifically, their goal of developing nuclear arms. Gray area exists here, not only in terms of chivalry, as the attack is thought to have been spread via USB memory sticks and the code itself designed to remain hidden and mask its effects on the system, but also in terms of the anonymous origins of the attack. While arguments can be made in terms of this approach being favorable to the aerial bombing campaign that Israel formerly sought U.S. support for and the military necessity of keeping Iran from developing nuclear arms, the proportionality of this attack could be a potential issue if indeed what has occurred up and until Spring 2011 is only the beginning of a larger campaign as some have suggested.

Despite previous efforts to mitigate the potential destructive effects of new weapons in the realm of international war law, Banks (2001) argues that specific changes are not likely in the face of information warfare, and that instead, these new weapons and tactics will be judged based on their closest analogs for the foreseeable future (p. 21). Further, ambiguities exist in justified reprisal to information war, particularly, he notes, due to reprisals generally being understood in reaction to physical attacks. If a more traditional conflict is instigated by information war tactics, as could be the case with Stuxnet, would retaliation in a more traditional sense be deemed an appropriate response? Banks cites additional challenges, such as the potential for information war to affect civilian populations in unanticipated ways, i.e. the long held belief that these tactics may not be able to target specific sites or predict effects. Though issues of proportionality are related to the principle of "humanity" which "requires the military commander to consider the possibility an attack may cause unnecessary suffering and/or superfluous injury, particularly on the civilian populace," strategies in targeting dual-use infrastructure are increasingly important in military strategy (p. 25). Concerns that

information-based attacks could have wider effects on civilian populations is also a concern in infrastructure war, though as Graham (2005; 2010) points out, the generation of second and third-order effects (specifically those that affect civilian attitudes toward leadership) is increasingly central in Air Force strategies such as Shock and Awe.

The main concern that Banks addresses in relation to cyberwar is proportionality and the potential for overkill through disproportionate use of force in untested methods of cyberwarfare. At the same time, he notes that the argument can also be made that in some cases, an information-based attack can be more humane. Such may be the case with Iran, where the alternative to Stuxnet is suggested to have been bombing the facility at Nantz. Banks writes:

> If, for example, the commander does not know the full extent of the enemy's information defenses, he or she could reasonably opt to increase the 'cyber ordnance' assigned to a target to produce the desired results… [Though too] much additional 'ordnance' could run afoul of war crimes law under the principle of proportionality. (p. 24)

Thinking about Stuxnet in terms of cyber ordnance rather than as a tactic of information war is useful, particularly insofar as it situates the code itself as a tool rather than the strategy of war, and more importantly, as a military rather than a political action.

Unlike an "ordinance," which the Oxford English Dictionary defines as "[s]omething decreed, ordained, or prescribed" and linked with the "decree of a sovereign," "ordnance" refers to the supplies and tools of war, from stores to bombs (2010). Ordnance has been used to refer to catapults, mounted guns, and other weapons used to fire ammunition, and perhaps in the context of emerging digital delivery mechanisms it will also refer to cyber weapons. The other important part of this term is "cyber," used both to describe the means and outcomes of network technology (as in "cyberinfrastructure" and "cyberculture") and the

mediation of everything from shopping to warfare on networks. The question of "cyber ordnance" is this: do we imagine "cyber" as acting as a site of warfare, or rather, a new way in which warfare is mediated? The ability for information weapons to target material objects, processes and sites suggests that, like aerial combat in WWII, cyber-mediated tactical strikes will radically refigure the battlefields of tomorrow. Virilio (2008) argues in *Bunker Archeology* that "if the *reduction* of obstacles and distances has always been the central problem of military space, we have reached today the rupture point: the distinction between vehicle and projectile has ceased" in the *coalescence* of the projectile and the vehicle "that cybernetics will purify by getting rid of the human factor in weapon systems" (p. 18). While Stuxnet represents such coalescence, the "human factor" is still very much involved in the process, though at the level of design and not in direct delivery to the site. In cyber war, the reduced distance between the vector and the weapon imposes a new set of challenges to defense.

Next, I turn more specifically to critical infrastructure, which began as a way to talk about those infrastructures essential to modern life and later became a way of identifying infrastructure as a site of security. Tracing infrastructure and cyber security efforts over the past 25 years via an examination of "critical infrastructure," I will provide insight into changing notions of criticality and a shift in responsibility for security. Particular emphasis will be put on communication infrastructure, which is central in the informationalized infrastructural ideal.

Defining Critical Infrastructure

In a report for congress titled "Critical Infrastructure and Key Assets: Definition and Identification," Moteff and Parformak (2004) explain that the meaning of critical infrastructures, though defined in various strategies and reports, is still evolving and open to debate and due to the broad nature of the term, "infrastructure" should be considered contextually. Their central goal is to chart changes in the meaning of critical infrastructure from initially referring to public works to a later (in part due to growing concerns about terrorism in the 1990s and then post-9/11 political climates) use of the term to refer to issues of homeland security.

When discussing infrastructure in the mid-1980s in terms of adequacy, everything from the materials to systems and institutions were considered "infrastructure." Moteff and Parfomak (2004) cite a Congressional Budget Office (CBO) report that considered infrastructure in terms of high capital cost and investment on the part of government, though they point out that the government has rarely implemented comprehensive legislation that defines infrastructure across sectors (taking instead a sector-specific approach). They note, however, that a 1984 bill enacting the National Council on Public Works Improvement targeted a wider scope of infrastructures from roads to space and communication facilities and federally assisted housing (pp. 2-3). Infrastructure here is a broad set of resources to be monitored and improved to provide better services.

In the 1990s, concerns about international terrorism led to a shift in focus concerning infrastructure in terms of questions of security. Moteff and Parfomak reveal how the broadened definition of infrastructure in Executive Order (EO)13010, an order which established the President's Commission on Critical Infrastructure Protection (PCCIP) in

1996, remains resonant with the multi-sector definitions of the 1980s, but takes a step beyond multi-sector concepts of infrastructure by identifying critical infrastructures, including the identification of some privately-owned infrastructures as critical. These infrastructures included telecommunications; electrical power systems; gas and oil storage and transportation; banking and finance; transportation; water supply systems; emergency services; and continuity of government. (pp. 3-4). The EO defined infrastructure broadly as:

> The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. (EO 13010)

Presidential Decision Directive 63 (PDD-63): CI Pre-9/11

Based on the final report of the PCCIP, President Clinton signed Presidential Decision Directive 63 (PDD-63) in May 1998, which called for establishing capability to protect critical infrastructures over the next five years from material and cyber threats, defining critical infrastructure as: "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private" (PDD-63, p. 1-2). Citing increased networking as increasing levels of interdependence between systems due to information technology, the directive urged the assessment of infrastructure vulnerability to natural destruction, failure, error, and attack:

> Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy. (PDD-63, p. 22)

Citing a historical precedent for government assurance of CI, the document stresses the U.S. government's intent to "swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems" (p. 2). The goal set in the PDD is that by 2003, the U.S. would both be able to protect CI from *intentional acts* (attacks) that would:

> …significantly diminish the abilities of: the Federal Government to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services… [and] the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services. (PDD-63, p. 2)

The directive references federal, state, and local government as well as the private sector and their respective roles in national security, safety and service, but does not explicitly discuss the community, family, or individual. The citizen is absent as well: instead, the object of safety, security, and service is the "public," "nation," and "economy." The directive presumes attacks on CI would center on government and economic targets, and proposes a public-private partnership (PPP), which, in the spirit of cooperation, would "seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector" (1998, p. 3). The structure outlined in the document essentially consists of a binary arrangement for each major CI group, which includes a Sector Liaison Official appointed from a government department (at the Secretary level) and a Sector Coordinator from the private sector. According to the directive, this pairing would create a Vulnerability Awareness and Education Program for each sector and contribute to a larger National Infrastructure Assurance Plan through:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;

- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack. (Directly from PDD-63, p. 3)

The development of sectoral plans (plans organized by industry sectors) would be overseen by a National Coordinator, Sector Liaison Officials and a representative from the National Economic Council. In addition, the directive calls for Special Functions lead by departments of the USFG to head up areas such as national defense and intelligence. A Critical Infrastructure Coordination Group (CICG) chaired by a president-appointed National Coordinator for Security, Infrastructure Protection and Counter-Terrorism isto report to the Assistant to the President for National Security Affairs. In addition to this group, the directive outlines a second group – the National Infrastructure Assurance Council – comprising state and local government officials as well as infrastructure providers. The plan accounts for Federal, state and local officials as well as infrastructure providers, but no specialists, researchers, or citizens. Federal departments and agencies are tasked with creating their own plans for protecting CI, which were then to be reviewed by the CICG.

In a series of guidelines for addressing vulnerabilities, one guideline in particular returns to the issues raised earlier in regard to the favoring of economic and private concerns over citizens, though it requires unpacking:

> The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, providing information upon which choices can be made by the private sector. These incentives, along with other action, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security. (PDD-63, p. 4)

Talk of economic incentives and a promise of avoiding direct regulation indicate favoritism for corporations: direct regulation will be used only in the case that the market fails to account for the health, safety, and well-being of the American People. The process is incentivized economically, and regulation is in contrast clearly only a "stick." Another guideline poses similar issues when it speaks of privacy: "Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably" (PDD-63, p.5). Here, the privacy discussed is that of consumers and operators, but not citizens. Along with establishing the Critical Infrastructure Coordination Group, producing Sectoral Vulnerability Awareness and Education Programs and contributing to a National Infrastructure Assurance Plan, the directive authorizes the FBI to expand a government National Infrastructure Protection Center (NIPC) and encourages the creation of a private sector Information Sharing and Analysis Center (ISAC).

Critical Infrastructure (CI) in a Post-9/11 Environment

After 9/11, two executive orders (EO-13228 and EO-13231) re-organized responsibilities for protecting critical infrastructure in the homeland. The first of these, signed October 8, 2001, EO-13228 established the Office of Homeland Security and the Homeland Security Council, precursors to the Department of Homeland Security, which was formally established as a cabinet level department in November 2002. Moteff and Parformak explain that this order is "noteworthy for its specific inclusion of nuclear sites, special events [large gatherings], and agriculture, which were not among the sectors identified in PDD-63" (2004, p. 6). This order amended President Reagan's 1988 EO 12656 titled "Assignment of

emergency preparedness responsibilities" and was later amended in the process of establishing the Department of Homeland Security in 2001 and 2002. Essentially, this order set into motion EO 13228, which established the Office of Homeland Security "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks" and a Homeland Security Council to advise the President on matters of homeland security (Executive Order No. 13,228, Section 2).

A second order, EO13231: Critical Infrastructure Protection in the Information Age, was signed just over a week later on October 16, 2001, and was concerned with the significance of information infrastructure for a range of other infrastructures, which are interlinked with, managed, and controlled by information infrastructures (Executive Order No. 13,231). The order revokes President Clinton's 1999 EO 13130 that established the National Infrastructure Assurance Council, creating instead the President's Critical Infrastructure Protection Board, which is responsible for outreach and information sharing with the private sector and state and local governments, incident coordination and crisis response, recruitment and training of executive branch security professionals, research and development, coordinating with law enforcement on issues of national security in the areas of cybercrime and critical infrastructure, international information infrastructure protection, advising on legislation relating to information systems for critical infrastructure, and coordination with the Office of Homeland Security. The Order explains that members of the board would be drawn from cabinet-level executive branch officials and in addition to Attorney General, the Chief of Staff, Chairman of the Joint Chiefs of Staff, Chief of Staff to the Vice President, Administrator of General Services, the Directors of the CIA, FEMA, OMB, Science and Technology Policy, and NEC, and the Assistants to the President for

National Security Affairs and Homeland Security as well as other officials designated by the president (Executive Order No. 13,231 section 6, a, i-xx). The Board's Coordination Committee consists of:

- Director, Critical Infrastructure Assurance Office, Department of Commerce
- Manager, National Communications System
- Vice Chair, Chief Information Officers' (CIO) Council
- Information Assurance Director, National Security Agency
- Deputy Director of Central Intelligence for Community Management
- Director, National Infrastructure Protection Center, Federal Bureau of Investigation, Department of Justice
- A *representative* may be appointed by the Chairman of the Federal Communication Commission (FCC) (Section 6, b)

In addition to these Executive Orders, CI is addressed in the USA PATRIOT Act of 2001. The Patriot Act addresses the interconnectedness of such infrastructures and the central role that they play in commerce, government, and security, a definition which was again referenced in the Homeland Security Act of 2002 that established the Department of Homeland Security (DHS). The *National Strategy for Homeland Security* (NSHS) of 2002 expands the definition provided in the Critical Infrastructure Protection Act, giving explanations for CI sectors and pointing to the potential for cascading effects; cyberinfrastructure, here, is an important but distinct CI element (Moteff and Parfomak, 2004). In addition, the NSHS also introduces for the first time a subset of *key resources— key assets*—which are targets that, if destroyed, "would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence" such as prominent monuments/icons, symbols associated with the United States as a Nation, and local facilities with destructive potential/value to local communities (Moteff and Parfomak 2004, p. 8). The 2003 *National Strategy for the Physical Protection of Critical*

Infrastructures and Key Assets (NSPP) further delineates categories for key assets: 1) monuments, symbols, and icons; 2) facilities and structures that represent economic power/technological advancement; and 3) structures "where large numbers of people regularly congregate to conduct business or personal transactions, shop, or enjoy a recreational pastime" (Office of the President. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* February, 2003. p 71, cited in Moteff and Parfomak, 2004 p. 9).

While Executive Orders shortly after the events of 9/11/01 superseded EO 13130, it was not until December 17, 2003 that the presidential decision directive that provided a framework for protecting critical infrastructure—PDD-63— was superseded. Homeland Security Presidential Directive 7 on the subject of Critical Infrastructure Identification, Prioritization, and Protection, formally adopts critical infrastructure and key assets as defined in the Homeland Security Act and adopts the categories for key assets put forward in the NSPP. In addition, the HSPD-7 revises the list of critical infrastructure sectors and the associated federal agencies to account for the creation of the Department of Homeland Security as a cabinet-level department, shifting responsibility for information technology, telecommunications, chemicals, transportation systems (mass transit, aviation, maritime, ground, surface, and rail and pipeline systems), emergency, and postal and shipping services to the newly formed Department of Homeland Security in protecting these critical infrastructure sectors. HSPD-7 adds to CA prioritization another focus on prioritization—health and safety—in its call for the Secretary of the Department of Homeland Security to "identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause

catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction" (HSPD-7 Section 13).

Currently, the Department of Homeland Security defines critical infrastructure as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof" (DHS website, 2011). Key resources are defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government." The site explains that Critical Infrastructure and Key Resource (CIKR) protection is crucial in that: 1) attacks can have negative effects on government and business operations and have ripple effects to outside of the target sector; 2) attacks and natural/manmade hazards can cause loss of life, property, the economy, and morale; and 3) attacks using CIKR as weapons of mass destruction could be devastating both at a material level as well as on the nation's morale. These are, in summary, the three points that the site highlights as being important in the mission to protect CIKR and represent the flip-side of military doctrines of infrastructure warfare (such as Shock and Awe), which seek to generate second-order effects, including (but not limited to) the destruction of dual-use (military and civilian) infrastructures. The Department of Homeland Security identifies 18 critical infrastructure sectors on their website as of Summer 2011: Agriculture and Food; Banking and Finance; Chemical; Commercial Facilities; Communication; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Transportation Systems; and Water (DHS, "Critical Infrastructure," 2010).

One of the key issues in assuring critical infrastructure protection has to do with categorizing critical and non-critical assets in each of these sectors. Moteff and Parfomak (2004) explain that in 1999 the Critical Infrastructure Assurance Office (CIAO) expressed concern that federal agencies tasked with CI responsibilities "lacked a clear understanding of what constituted a 'critical asset' within an infrastructure" (p. 11). While the "key asset" category under CI is meant to serve as a way in which to prioritize a subcategory of key resources which include "individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence" such as historical and cultural sites and facilities such as power plants and dams, the 2002 *National Strategy for Homeland Security* adopted "critical assets" as a way of thinking about protecting those elements most critical in critical infrastructure (DHS cited in Moteff & Parfomak, 2004, p. 8).

DHS and Communication CI

Of the critical infrastructure sectors identified by the DHS, the communication sector is the most vital to processes of informationalization ("smart") and serves as both a site of and a vector for cyber-attack. In discussing the communication sector, the DHS website highlights both the crucial role that communication plays in business, public safety and government activity, and stresses that the communication sector must be thought of in terms of the full range of services beyond voice, including interconnected multiservice technologies operating on satellite, wire line, and terrestrial wireless networks. While these networks are mostly privately owned, they are considered essential for public safety, the economy, and the operation of government at multiple scales. The DHS stresses cooperation with the private

sector on issues of security on these networks, which are closely tied with a range of other infrastructure sectors including energy, information technology, banking and finance, emergency services, and the postal and shipping sector (DHS 2010b). In identifying CKIR protection issues in the communication sector, the DHS National Infrastructure Protection Plan for the Communications Sector notes that "While it is unlikely that the loss of a single communications facility or key node would significantly impact the Nation's communications system, the loss could have cascading impacts on other critical infrastructure" (2010b, p. 2). The document explains that efforts to reduce risk have centered on the security, resilience, and restorability of communication networks as well as risk assessment of cross sector interdependency with communication networks for "high-risk assets, networks, systems, and functions" (p. 2)[3].

The risk of cascading system failure is perhaps the most significant downside to smart infrastructure: while information layers facilitate remote control, dynamic manipulation, and visibility to processes, the same capabilities make infrastructures vulnerable to more extensive consequences of failure and/or attack. For instance, if communication services were to be disrupted, the Better Place electric vehicle platform would be crippled: drivers would be unable to use the functions of their cellular phones as remotes for their vehicle, grid operators would be unable to see where power was being used or stored in vehicles, key fobs would not be recognized at public charging stations, and card readers at public charge stations would be unable to validate accounts to charge for the "charge."

[3] More detail for specific elements of the plan for the communications sector is outlined in the Department of Homeland Security Communications Sector-Specific Plan, a 126-page document that serves as an annex to the National Infrastructure Protection Plan (2010b).

The notion of public-private partnership (PPP) pervades the National Infrastructure Protection Plan in the 18 critical infrastructure and key resource sectors identified, placing the lion's share of security responsibility on industry with little government oversight or regulation. At least as far back as PDD-63, the prioritization and protection of critical infrastructure has been addressed in terms of a PPP that has continued to be present in efforts to secure and protect critical infrastructure. Given the essential nature of communication infrastructures in economic exchange, public health and safety, and government operations, plans for securing communication CI should be simultaneously in the best interests of the market, the people of the United States, and state, local, and federal governments. One challenge to such cooperation is the obvious concern that profit motives can interfere with the charge to assess criticality.

Take, for example, the microcosm of the home, in which a variety of essential and costly infrastructures are necessary to maintain the space as both a safe and comfortable place to live. Before buying a home, a prospective buyer may ask about the condition of the foundation, wood (termites), roof, central air conditioning and/or heating unit, kitchen appliances, and water heater. While they may not make the "components to consider" short list, less costly components of the home are much more critical to the operation of the home, such as a door to the outside. Though the cost of repairing or replacing a door can be much lower than that of a water heater, the door is more essential to keeping food, people, and belongings safe from the elements, animals and insects, and intruders. Ultimately, the cost of replacing a door makes it a less of an issue than other aspects of the home investment despite its criticality in terms of security.

In the case of the door, homeowners could either purchase a high-security blast-proof fire-safe door upon moving into a new home, or choose to keep any number of replacement doors in storage on premises to prepare for rapid restoration of home security in the event of door failure. The decision could be made after completing a risk assessment and cost-benefit analysis of both options. Similar cost-benefit analyses impact industry efforts to define key resources and key assets, and like our brief example with what we might at first consider "key assets" of the home, it is crucial that we make a clear distinction between criticality and expense. Often expensive components are critical in proper system function, but when responding to a crisis or preparing for one, criticality needs to be examined apart from cost. The DHS Information Analysis and Infrastructure Protection Directorate (IAIP) has been charged with the mission of making such classifications more uniform and establishing a database of key assets, but because the PPP is central to the U.S. approach to protecting critical infrastructure, paying continued attention to industry efforts to co-construct the meaning of what is and what is not a "key asset" is essential.

Many measures to ensure usability of our communication, information and electrical infrastructures include a focus on rapid restoration of systems in addition to securing systems in the event of attack or failure. As an example, in discussing the effects of electromagnetic pulse (EMP) on the electric grid, Eric Hsieh (2010) explains that an EMP will damage anything that uses semiconductors, such as electrical transmission and distribution infrastructure. While he explains that most power equipment can handle voltage levels associated with EMP, voltages as low as 50 volts can melt the silicon on a chip. As chips are increasingly incorporated into electrical networks in efforts to increase control capabilities, an EMP would result in a loss of the advantages of informationalizing electrical transmission

and distribution infrastructure. In a podcast for NEMA, a trade association representing electrical and medical imaging equipment manufacturers, Hsieh explains that an EMP has three stages: initial blast, induced currents, and direct current through the Earth's crust. In the first stage, the initial blast of an EMP results in high electrification that can damage equipment, particularly sensitive silicon chips. The main defense against the initial blast is EMP shielding, which while effective, is also very expensive given the number of components that would potentially need to be shielded. For this reason, Hsieh (2010) suggests that components should be assessed based on replacement cost, and components less expensive to replace than shield should be stockpiled in a safe location and replaced after an EMP in efforts to rapidly restore the grid. The second stage of EMP, in which currents are induced as the electromagnetic field spreads over land, can be picked up by transmission lines and can be mitigated by surge arrestors. The third and final stage, in which direct current travels through the Earth's crust, is not as harsh as the similar effects that solar storms have on the same infrastructure, he explains, and can be mitigated by installing breaks between devices and the ground (Hsieh, 2010). Solutions for recovering from electromagnetic pulse, then, take a simple approach: continue to solve for the certainties of solar storms and power surges, and maintain a backup of important but inexpensive components that enable smart grid capabilities. We consider electricity and communication to be critical, but not smart systems (at least not yet), as they are currently generally limited in their deployments or seen as a value-added "perk." With so much falling under the umbrella of critical infrastructure, the issue of appropriate assignment of criticality is… critical. Without clear standards for what constitutes CI, too many or too few infrastructures might be protected, leading to either an issue of resources or security spread too thin.

Given the centrality of communication infrastructure in developing smart grids, smart transportation, and contributing to the creation of a "smarter planet," attention to this sector is of critical importance. I next review the pre-Stuxnet environment, particularly as it concerns computer crime in the USA PATRIOT Act in regard to imagined potentials and possibilities of hacking, cybercrime, and cyberterrorism. While Stuxnet is said to represent the first real computer-mediated threat to physical infrastructure, fears of material violence via computer networks have long been used to legitimate increased vigilance of computer hacking and (later) cybercrime and cyberterrorism.

Cybersecurity: The pre-Stuxnet Environment

While the effectiveness of the Stuxnet worm and recent attacks on Pentagon information systems have generated a renewed focus on addressing cyber threats, these initiatives can be understood as part of a much longer history, and rather than synthesize the dispersed initiatives of the executive branch concerning critical infrastructure and cybersecurity, I will review a brief history of computer crime law in order to understand the reframing of computer hacking in terms of cyberterrorism after 9/11. In many cases, the potential for computer crime to affect the regular operation of essential infrastructure was leveraged in order to call for heightened security efforts as well as increased penalties for crimes on information networks. Though the belief that cyberattack could result in material damage seemed far-fetched prior to Stuxnet, mere speculation of such capabilities was leveraged to demonize hackers, fuel the computer security industry, and support the PATRIOT ACT.

Discourses surrounding computer hacking are varied, and conflict over what hackers are and what hacking is has been further complicated by cybercrime, cyberterror, and cyberwarfare. While the hacker has previously been described through a broad range of metaphors—cowboy, joy rider, terrorist, drug addict, murderer, and sexual deviant (Chandler, 1996; Taylor, 2001; Weintraub & Kerstetter, 2003; Halbert, 1997; Best, 2003)—new images are less abstract. More information has become available concerning specific attacks, vulnerabilities exploited, security measures, reach, and effect. The hacker image has also become more diverse, with popular images ranging from the classic young white male computer enthusiast (*War Games*, *Hackers*, Kevin Mitnick) to faceless groups (from terrorists to *4chan's* Anonymous) to glamorous stories of the hackers of Râmnicu Vâlcea, a small Romanian town also known as "Hackerville," full of high-end cars and luxury items (Bhattacharjee, 2011).

While "hacker" may have lost some of its shock value as Internet and mobile device adoption began to reach market saturation in the U.S. in the late 2000s, a level of dependence on such technologies and networks has made attacks more serious, as is reflected in shifts to language like "cyberterrorist" and "cybercriminal" as well as an increased link between system breaches, viruses, and worms with more traditional crime. A concurrent move in the ways in which computer crime is discussed reflects a better understanding of the nature of these acts, as language is increasingly specific and reflective of traditional crime: identity theft, unauthorized access, system breach, circumventing security measures (DRM), etc.

Legislative work to curb hacking began mainly in the Computer Fraud and Abuse Act (CFAA), the Electronic Communications Privacy Act (ECPA), and the Stored Communications Act (SCA) all in 1986. As with the Digital Millennium Copyright Act

(DMCA) in 1998, designed mainly to prohibit the circumvention of Digital Rights Management (DRM), legal descriptions of computer crimes centered largely on issues of protecting information, whether in terms of intellectual property, sensitive government and military information, or the security of financial markets in an increasingly networked economy. Post-9/11, a developing Homeland Security mentality enabled a series of additional restrictions to come into effect, placing hacking in a larger discussion about safety as well as the security of the nation. Crimes on computers no longer took place on information networks alone: children were at risk of being stalked by pedophiles, bullied by classmates, and were beginning themselves to engage in illegal activities, such as sexting (sending sexually explicit messages), over information networks. These crimes are not what we would consider hacking or computer crimes, but these and other threats facilitated by information networks had the effect of legitimating increased focus on computer activity. Though these crimes are still a far cry from the scenarios depicted in *Wargames* (1983), where mutually assured destruction was threatened via information networks, or *Live Free or Die Hard* (2007), where the United States is brought to its knees through a sophisticated multiple infrastructure attack, material consequences of computer-mediated crime were significant enough to be addressed in the USA PATRIOT Act.

Passed October 26, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) is one of the most significant pieces of law passed in the U.S. in the past 25 years in terms of its scope and gravity: it not only impacts the ability for the U.S. to combat terrorism, but also everyday crimes, many of which now fall under new broad definitions of terrorism. Despite the fact that the 9/11 attacks that led to passage of the act were not directly

facilitated by cyber tactics or techniques, the Act contains much in the way of addressing cyberterrorism and computer crime in terms of criminal laws against terrorism and updating laws to reflect new technology, and has had a substantial effect on the body of computer crime law. Due to the speed with which that the Act was passed—President Bush signed the Act on October 26, 2001, less than two months after the 9/11 attacks—some provisions were included in the Act with a sunset clause.

Though many of the provisions concerning computer crime were scheduled to expire at the end of 2005 due to sunset provisions, early 2006 saw those laws become permanent; officials argued that letting the provisions expire would place the rights of criminals over those of victims and thwart efforts to combat hacking and cyberterrorism (Gonzalez, 2005). One place where arguments for making these provisions permanent can be located is within a 2004 Department of Justice (DOJ) report—"Report from the field: The USA PATRIOT Act at Work"—that reviews ways in which the Act had been instrumental in combating terrorism and other crime. Throughout, computer crime is framed as violent crime (kidnapping, hate crimes, abuse) whether to the end of demonstrating the effectiveness of the USA PATRIOT Act or of a larger aim to increase penalties and punishments for computer crime in the future.

Cyberterrorism is discussed in the report as part of a broader argument for the relevancy and necessity of the Act in strengthening criminal laws against terrorism. Though the report does not provide a specific definition of cyberterrorism, it details efforts from doubling maximum penalties for intentionally damaging federally protected computers to eliminating the need to establish financial damage to prove liability by adding a fifth category of any damage to "a computer system used by or for the government in furtherance of the administration of justice, national defense, or national security" (United States

Department of Justice, 2004, p. 13). This broadens the scope of federal protection, ensuring "that those who intentionally invade and damage computer systems are held responsible for the full economic consequences of their actions" regardless of a system owners' ability to establish these damages at a specific threshold (p. 14). A section of the report, titled "Updating the Law to Reflect New Technology," discusses the Act in terms of arming law enforcement with the tools to cope with new technology, explaining that the U.S. is "waging a 21st century war with mid-20th century weapons" (p. 18). The changes fall into three categories: new tools to fight terrorists; enhancement of wiretaps and pen register and trap and trace devices (which record the numbers of outgoing and incoming calls, respectively); and third party cooperation.

The first subsection, "Providing New Tools to Fight Terrorists and Criminals Using Electronic Forms of Communication," cites terrorist and criminal use of the Internet, and provides examples of cases where provisions of the Act have helped law enforcement "keep pace with terrorists and other criminals" as well as combat sexual abuse of children. A few incidents where the act was used to gather information are highlighted, including the halt of a "Columbine- like attack that was supposed to occur on a specific date in early March 2004" (p. 19). The provision allowed law enforcement to obtain the identity of the individual in time to procure a confession before the event could even take place. The Act has also made operations possible that dismantled rings of active child molesters and pornographers; those operations were responsible for the rescue of over 100 child victims and 24 convictions in the United States (DOJ, 2004).

Through "Enhancing Existing Investigative Tools" including amendments to the pen register and trap and trace statutes, it became less difficult to track the communications of

international terrorist conspirators, domestic terrorists, major drug distributors and thieves able to obtain bank account information and burgle accounts. According to the report, the extension of the Pen Trap Statue has disrupted a plot to use cocaine to purchase Soviet bloc weapons for the United Self Defense Forces of Colombia (designated a foreign terrorist organization by the State Department). The report stresses that the Act has also proven useful in catching and arresting "phishers" (who deceive persons through various electronic means with the goal of obtaining sensitive personal and financial data) and punishing hacker groups that shut down internet service providers (ISPs). The statute allows investigators to obtain information in real-time, before records are destroyed.

The last subsection of the argument for the Patriot Act's relevance to security from cyber-attack is the "Cooperation of Third Parties." Enhancements falling into this section allow electronic communications service providers to disclose records to the government in situations involving an immediate danger of death or serious physical injury to any person without the threat of being sued. The report calls this crucial in the investigation of a bomb threat against a school, the apprehension of a man threatening to burn down a mosque, in cases involving abducted or missing children, and in rescuing an 88 year-old Wisconsin woman who was kidnapped and held for ransom. "When the victim was found," the report goes on, "she was bound in an unheated shed during a cold Wisconsin winter several feet from a suspect's residence" (DOJ 2004, p. 28).The Act also allows ISPs to "enlist the help of law enforcement to monitor the activities of hackers who unlawfully access their computer networks" (DOJ 2004, p. 28), allowing victims of computer crimes to ask law enforcement to monitor trespassers on their systems.

The way in which cyberterrorism and hacking were operationally defined in the USA PATRIOT Act as a part of the "war on terrorism" established grounds for the U.S. Government to define hacking as terrorism in their own terms. Despite no evidence of hacking directly resulting in terror and/or physical violence, the report and the USA PATRIOT Act construct the hacker as a threatening enemy, violent criminal, and terrorist. While in 2004 (and later in 2006 when these provisions were made law) there was no evidence of cybercrime resulting in direct physical effects (though attacks often have consequences in terms of security costs, data loss, and software patching), government discourse certainly mobilized such concerns to legitimate an extension of the "hacker crackdown" of the mid-1980s under the aura of terrorism. As Packer notes in *Mobility without Mayhem: Safety, cars and citizenship* (2007), "The spectacular accident, whether a mistake or purposive, has continually been used to legitimate the safety apparatus and, post-9/11, the security apparatus" (p. 15). In addition to exposing system failures, he explains, such accidents can serve as models for how to accomplish attacks. As a spectacular accident of informationalized infrastructure, Stuxnet serves as a free-floating legitimator for heightened security, surveillance, and screening on information networks (though as yet it has not served as an argument for disconnection).

Smart Security and the Public-Private Partnership

Stuxnet requires us to rethink connection, defense and security. Virilio (1994) writes that after the aerial bombing campaigns of WWII, walls lost their old power to defend, and that "[i]t was no longer in distance but rather in burial that the man of war found the parry to the onslaught of his adversary; retreat was now into the very thickness of the planet and no

longer along its surface" (p. 38-39). Where is there to retreat from globally connected information networks in informational society? With cyber ordnance now proven, getting the balance right between the dual demands of military and financial securitization is a key area to examining “smart” strategies of connection in a new infrastructural ideal. Despite the established criticality of communication infrastructures in the United States, informationalization continues to reorganize essential services such as transportation and utilities. Rather than question whether or not information *should* be added to these processes, the focus has been on *how* to do this, while mitigating (rather than eliminating) risk in terms of vulnerability to direct physical attack or cyber mediated weapons.

Current Department of Homeland Security efforts and prior efforts to secure critical infrastructure (such as PDD-63) stress the importance of the public-private partnership in the protection of critical infrastructure, placing responsibility and oversight largely with the private companies under the assumption that such organizations not only have the most expertise in their respective sectors, but also that they have a responsibility to protect their investments and will take appropriate security measures to do so. Without coordinated oversight of such activity, the private sector wields tremendous influence over the security of critical national infrastructures, and, following this, the security of the nation itself. While moves to deregulate across the board have generally been discussed in terms of trends toward neoliberalism, shifting responsibility to corporations to secure the United States and its infrastructure from terrorist attack and acts of war represents a new period in the history of national defense.

This move can be seen in larger trends in government to utilize contractors both at home and abroad to carry out military operations and domestic security. In the case of

Stuxnet, evidence points to cooperation between Idaho National Laboratories and the German company Siemens (whether they knowingly facilitated the attack is unknown), calling into question how the United States government can make the public-private partnership work when corporations (and in some cases, governments) are increasingly global. If a Swiss company were to have created the control units, would the generally neutral status of their home country have prevented such cooperation? If they were to refuse to cooperate, would action be taken against them? Will such dependence on cooperation with the private sector make foreign companies hesitant to enter U.S. markets (or on the flip side, make the government hesitant to allow companies from emerging economies to enter key infrastructure sectors)? How far will nations go to protect networks?

As noted previously, the "third age" of cybercrime leverages the global connectivity of communication networks and consistency of platforms as a vector for attack. Informationalization further intensifies the ability for attacks to be delivered via communication infrastructure as an increasing amount of critical infrastructures are brought into relation with one another. While these processes in part work to bring about a "smarter planet," they also create new battlefields for new kinds of "smart war." Discussing the centrality of speed in war and defense, Virilio (1994) indicates that infrastructure has a critical role: "[t]here is thus a hierarchy of speeds to be found in the history of societies, for to possess the earth, to hold terrain, is also to possess the best means to scan it in order to protect and defend it" (p. 19). Attention must be paid to the work done to secure these means of territorializing space, particularly as infrastructures are rendered "national" in their designation as critical infrastructures or key resources, even as they remain under the control of private corporations.

Having explored some of the "determinators" of informationalization by analyzing critical infrastructure in terms of the "organizations, institutions, or credentialized experts" (Packer, 2010, p.101) with the power to make truth claims about a phenomenon, in the next chapter I turn to *the grid*. Here I explore resistance and alternate discourses of connection and informationalization, particularly in struggles against the imperative to connect, or to remain connected against all odds.

Chapter 4: The Grid and the Smart Subject

With increased focus on the protection of critical infrastructures from threats in both the traditional and cyber-theater, the potential for disconnection through terrorism, war, natural disaster or failure has some individuals preparing for the worst. From transportation to energy, the balance between open, financially productive networks and secure networks is difficult to maintain: if too open, a network is vulnerable; if too secure, it is unusable. The security industry makes millions of dollars finding ways to secure systems, networks, infrastructures, facilities, resources and personnel through technological and procedural solutions that work to make these same assets accessible, marketable, and profitable. This is done through what Jeremy Packer and I have termed *technologies of screening*, which are those technologies and techniques which work to filter and sort the permissible, useful, and acceptable users of a network from forbidden, risky, and unsafe subjects (Packer & Oswald, 2010). A range of techniques can be used to accomplish this screening, from biometric filtering and document verification to algorithms that discern the potential for a driver to become dangerous based on driving behavior (Packer, 2008). Despite increasingly advanced technological methods and measures, security experts are unable to meet a standard of total security (much to the benefit of the insurance industry).

Despite prevailing discourses of connectivity and smart technologies, there are those who do not participate in the large interconnected system of systems, choosing instead to live "off the grid." Even some citizens on the grid prepare for potential disconnection—referring to themselves as "survivors" or "preppers"— and ready themselves with plans, provisions and structures in order to ride out periods of disconnection. For millions of others dependent

on the multitude of systems that compose the infrastructure of daily life, the grid going down would be devastating. This chapter examines the notion of "the grid," beginning with a brief return to smart networks as the new infrastructural paradigm before briefly discussing "off the grid" living in the United States as well as the depiction of post-grid scenarios in popular culture. In order to examine the centrality that the grid has come to occupy in the present day, this chapter undertakes an analysis of preparations and shelter design to demonstrate changing relations to infrastructure and threat in terms of that design. In examining the spaces that individuals prepare for disconnection from the grid, I will trace the changing threats and necessities from the Cold War to the present day.

Some scholars have argued that as our society becomes increasingly mobile, it is imperative to understand the systems that individuals use to move through, communicate, and make sense of space. In mobility studies, scholars such as John Urry have argued that the relationship between social ties and the material worlds that underpin them are complex and must be understood in part through the *immobilities*: the technologies, infrastructures, and places that make these relationships possible. In *Mobilities* (2007), Urry specifically identifies systems of immobility as including "wire and co-axial cable systems, the distribution of satellites for radio and television, the fiber-optic cabling carrying telephone, television and computer signals… and the massive infrastructures that organize the physical movement of people and goods" (2007, p. 123). Here I will examine a specific space of extreme immobility—the bunker—as a space designed to ensure later mobility (and an alternative to death and suffering) after a major crisis.

Though much research in communication focuses on cultural artifacts, discourse, and relationships, the ways in which we produce and distribute content and maintain relationships

are material. What is needed is to "place" infrastructure materially, to render it sensible in a way that would call attention to its existence. Looking at the spaces of survival does exactly that: it calls our attention to a unique articulation of space, infrastructure, and resources designed for a specific purpose. As survival shelters require vast investments of time and money, they represent significant investments which become relatively permanent after their initial construction (due to "sunk-cost" and "lock-in"). Langdon Winner writes: "…technological innovations are similar to legislative acts or political foundings that establish a framework for public order that will endure over many generations" (1986, p. 121). Careful consideration of these spaces will enable us to better understand survival in terms of what these spaces were designed to protect individuals against, who they were designed to protect, what life inside was imagined to be like, and what kinds of worlds were imagined both inside and outside of the bunker.

Most commonly understood as the electric transmission and distribution infrastructure, 'the grid' is increasingly used to refer to a variety of immobilities beyond the electric grid, from the new Duracell-branded personal wireless charging station to a general term used to describe the totality of infrastructure, systems, and networks that support industrialized life (Huler, 2010; Rosen, 2010). Understanding the use of the term as referring more broadly to networked infrastructure for the distribution of energy, information, and resources, this chapter explores the ways in which life after the grid is increasingly represented in shelter design as "grid away from the grid."

Looking at shelters through the lens of Lefebvre's spatial triad (1991), this chapter will focus on representations of life after the grid in order to reveal more about the nature of these "immobilities" (Urry, 2006). It explores the changing representation of infrastructure

failure by asking questions of both more traditional Cold War shelters and the new shelter solutions, asking: What do shelters serve as protection from? What flows enter and exit these spaces? How social are shelters/bunkers, and what form does social life in them take? What do they reflect about connection/communication and culture? My hypothesis is that an analysis of shelters will point to something of a "grid mentality" in solving the problem of survival in a post-event scenario. Examining the juncture between (im)mobility, crisis, and survival, this chapter will further develop understandings of what "the grid" has come to mean in American culture, particularly in terms of how the grid is framed in terms of survival. First, however, we must look at the grid itself in more detail.

On and Off the Grid

In his book *The Grid* (2007), author Philip Schewe looks at the history and development of the electric grid in the United States, explaining that "much of what we call modernity is fundamentally electrical in nature or at least dependent in a fundamental way on the electrical grid" (p. 13). Schewe explains that the electric grid was not inevitable, but that it constituted a better energy delivery system than the alternatives in the late 1800s such as steam or gas. In fact, he explains that the focus of the book is about the electrical grid, and that: "Electricity is, in essence, a form of bottled lightning. *The Grid* is partly about the bottle… and partly about the lightning" (p. 1). He explains that the electric grid is one of many other grids such as communication, water, and sewer grids, as well as a number of grids which have become obsolete, including ice delivery, hydraulic utilities, and horse feeding stations (p. 23-24). He explains later that *the* focus of the book is about those grids which send energy by wire, listing six "electrical –information gridlike inventions": 1)

telegraph, 2) telephone; 3) wireless; 4) radio; 5) computers; and 6) Internet. His focus lies mainly in looking at the ways in which the electrical grid is becoming increasingly interconnected, with information technologies, the economy, and other grids.

Author Scott Huler interprets the grid more broadly in his 2010 book *On the Grid: A Plot of Land, an Average Neighborhood, and the Systems that Make Our World Work*. Focusing largely on the infrastructures that support his everyday life in Raleigh, North Carolina, Huler looks to a range of grids from power generation and transmission to water and sewer, transportation, land surveying, and landfills. Throughout, Huler glorifies the vast, connected, and amazing infrastructure required to facilitate contemporary American life while discussing grid dependency and arguing that we should be paying more for our utility service both through what we pay to utilities and what we pay in tax dollars. After reading his book about the wonders of infrastructure, or seeing him talk about it, it is difficult not to be awash in wonder at how it all operates, how many individuals and companies are involved in the invention, deployment, provision and maintenance of services, and the fact that they are nearly always available… until they aren't.

In an interview discussing his book *On the Grid* (2010), Scott Huler made a point to mention that no one gets elected on a platform of repairing roads, but rather one of building new roads and breaking ground on new projects. Likewise, Graham (2009) discusses the ways that "infrastructural mega projects" are ones linked to progress and often serve as signs of progress, which, combined with the notion of linear history (that we progress only by moving to a new "age" through our tools, materials, and technologies) obscure the importance of the less glamorous infrastructures. For this reason, he suggests that rather than thinking of infrastructures as supplanting one another, scholars should look to the ways in

which infrastructures evolve and relate, using the example of a new fuel pumps which, by allowing users to pay by credit card at the pump, exist at the intersection of the automobility, telecommunications, global finance, and petroleum markets. Huler has a similar interest in *On the Grid* about the garbage disposal, which he argues has an adverse effect on five systems -- fresh water, electricity, compost/landfill, sewage, and drain water, leading to a "lose-lose-lose-lose-lose situation."

In the edited collection *Disrupted Cities: When Infrastructures Fail* (2009), Graham argues that infrastructure provides the background for understanding modern urban life, and explains that the focus of his edited collection is to understand what happens when such invisible flows as are supported by infrastructure are interrupted by any means. The book accomplishes this through a series of case studies that look not only to national disasters and technical accidents, but also deliberate attempts to target the infrastructures of daily life. In focusing on moments of failure, the cases provide insight into the taken-for-granted circulations and animate infrastructure and socio-technical systems by showing what they look like when they are truly static. Graham (2009) explains: "Disruptions and breakdowns in normal geographies of circulation allow us to excavate the usually hidden politics of flow and connection, of mobility and immobility, within contemporary societies" (p.3).

Graham explains in *Cities Under Siege* (2010), and makes clear in his larger body of work on infrastructure warfare, that dependence on infrastructure means that everyday life is "stalked by the threat of interruption: the blackout, the gridlock, the severed connection, the technical malfunction, the inhibited flow, the network-unavailable notice" (p. 265). When infrastructures cease to be articulated in productive ways, they become useless to us, can direct no force, and can get us to no useful end. Graham points to examples such as the 2003

Northeast Blackout to demonstrate the ways people begin to focus on survival and satiating basic needs when infrastructure fails: finding warmth and safety, clean drinking water and food, dealing with the disposal of wastes, etc. Then, of course, there are those who choose in the first place to connect to the "grid" in a more limited fashion, sometimes making a deliberate choice to be "off the grid."

Nick Rosen's *Off the Grid* (2010) frames an increasingly infrastructure-dependent society as overbearing, dangerous, and undesirable. Sharing his experiences and conversations with individuals living off grid as part of the back-to-the-land movement, Rosen paints a picture of an alternative for those who are fed up with the "conveniences" of modern connected life. Looking for a group of like-minded people to live with who have "turned away from the hyper-consumption of the past thirty years, the pointless acquisitions, the hopeless materialism and the obsession with celebrity trivia" and land on which he could live without going too deep into debt, Rosen reveals that it is not his intention to be off the grid full time, but rather as a temporary escape from mainstream society (p. 12).

A 2007 documentary – *Off the Grid: Life on the Mesa*— takes on the difficult ethnographic project of examining a group of about 400 people living off the grid on "The Mesa," a 15 square mile patch of the desert of New Mexico. In the opening minutes of the documentary, a filmmaker rides along with a Mesa resident who explains what it is like to live on the Mesa, off the grid, by laws of the land established outside of the larger government apparatus. While it is difficult to imagine how someone "off the grid" manages to maintain an automobile, particularly when it comes to fuel, it soon comes to light that there is a very active barter economy fueled by marijuana that sustains many Mesa residents. One home featured in the documentary was even outfitted with solar panels which were

traded in exchange for marijuana. Cars, sparse generators and solar panels aside, the residents generally live in squalor. Many of those interviewed in the documentary were war veterans, some suffering from Gulf War Syndrome. Many self-identified patriots explained that living on the Mesa made them feel like they were in the last remaining part of America that is free. One inhabitant, explaining how isolated the area was, explained that "We don't dial 911, we dial 357… .357 Magnum." "Mama Phyllis," who prior to life on the New Mexico desert was a psychiatric nurse for 20 years, explains that the Mesa is the largest outdoor insane asylum, that "people come here for solitude because they can't find it out there." Another resident explains his reason for being there perhaps most simply: people on the Mesa "just want to be left the fuck alone." Those making a choice to operate off the grid in this capacity are clearly less affected by infrastructure failure in the ways that the majority of citizens of informational society are when the grids we depend on fail.

The Grid is Off

Even when one chooses to be on or off the grid (and to what degree), the fact remains that the grid is not foolproof, and sometimes – by attack, failure, or act of God— infrastructures can and do fail. As the much discussed August 2003 Blackout in the Northeast United States and more recent natural disasters such as the 2010 7.0 magnitude Haiti earthquake, the 8.8 magnitude earthquake in Chile in February 2010, and the March 2011 9.0 magnitude Tōhoku earthquake and tsunami in Japan demonstrate, on occasion the grid fails to be resilient. Even less eventful weather conditions have adverse effects on grid operation, from iced roads to limbs hitting power lines and those too-hot summer days that result in brownouts or rolling blackouts.

While Stephen Graham has discussed the intentional disconnection of urban infrastructure in *Disrupted Cities: When Infrastructure Fails* (2009) and his most recent book, *Cities under Siege: The New Military Urbanism* (2010), here I will look specifically to ways in which individuals prepare for extended stretches of immobility in anticipation of infrastructure failures. By planning and preparing for disconnection from the grid—through crisis scenarios and plans, guidebooks and bunker construction—governments, corporations, and individuals engage in an important process of representing space. In looking at changes in shelter spaces over time, I hope to illustrate a shift in both the nature of imagined threats as well as what constitutes survival during a crisis. While Cold War shelters and bunkers were designed to enable the nuclear family to survive the nuclear threat, shelter solutions such as those designed and constructed by the Vivos Group (2010) have been created to withstand everything from anarchy to super volcanoes and are designed as networked communities rather than nuclear units, with residential pods linked to common, storage, and medical areas.

Surviving in Popular Culture

From 1940s air raid drills to Cold War fears of all-out nuclear war and more recent threats such as Y2K, 9/11 and the 2012 conspiracy, no generation alive in the United States today has existed outside looming threats and faceless foes. One place to read the changing threat perception is in popular culture, specifically films which both express and reflect socially shared imaginaries about surviving after a disaster. What skills are valued, and what role do bunkers play? Zombie movies can be viewed as "survival guides" in many ways, as they center generally on modes of staying alive in a post-apocalyptic world where a fortification and bunker mentality is key to survival – the goal is rarely to defeat the enemy,

but to instead manage survival (*28 Days Later*, *I am Legend* and the series *The Walking Dead*). In zombie scenarios, protagonists are more mobile during daylight hours, hunkering down in abandoned houses, vehicles, and other makeshift shelters to survive the night.

Survival is a key element in a number of Cold War-Era films, notably *Dr. Strangelove* (1964), the NBC special *The Day After* (1983), and *Red Dawn* (1984), which all depict Americans struggling with survival in the face of the communist threat. While *Dr. Strangelove* focuses on the military industrial complex and vast underground government facilities, *The Day After* can almost be understood as a sequel, as Americans living out a normal day in the American Midwest are cast into fear and uncertainty as law breaks down and they struggle to survive in rural areas or crowded in universities and hospitals as an unseen government sends reassurance from a remote location. *Red Dawn* (1984) takes a different tack, and as small Midwestern towns are occupied by communist forces, this time the nuclear threat is absent; rather than destroying America, enemy forces want to take the nation as-is while an again-absent government supports a band of teen patriots from the wings. While some hunker down, it is those who are willing to put their lives on the line for god and country that are able to ultimately prevail and force out the communist threat through guerrilla tactics and sheer determination.

The wave of natural disaster films in the late 1990s can be seen as representing a shift in thinking about survival in a post-Cold War era. A slew of natural disaster films from *Twister* (1996) and *Dante's Peak* (1997) and *Volcano* (1997), *Deep Impact* (1998) and *Armageddon* (1998) postitioned the disaster movie as an ever wider threat increasingly out of human control – these films are about people coming together, sacrifice, nature's power to destroy and mitigating disaster through technology and ingenuity. But these films had a time

and place, and in the 1990s as the economy and technology boomed, there seemed to be nothing that money and technology could not make right. Even in *Independence Day* (1996), where a hostile race of aliens target major cities and seats of government, America's boy from the Midwest, armed with the most advanced technology, makes the ultimate sacrifice by making a Kamikaze run into an alien ship after Captain Steven Hiller (Will Smith) and David Levinson (Jeff Goldblum) disable the fleet's defenses with malicious code. Another focus in the 1990s (as biotech markets boomed) was disease. *Outbreak* (1995) and *12 Monkeys* (1995) reflected this concern, from the immediate effects of the Ebola virus popularized in the best seller *Hot Zone* (1994) to a larger growing global AIDS pandemic.

In the 2000s a different breed of survival media, reflective of a new state of exception brought on by the events of 9/11 and a growing fear of global threats became apparent, including pandemics as in *28 Days Later* (2002) and *Children of Men* (2006); terrorism as most clearly depicted through eight seasons of *24* (2001-2010) and *Live Free or Die Hard* (2007); and the unknown consequences of type-2 climate change as in *The Day After Tomorrow* (2004) and *2012* (2010). Even more abstract are films and television programs that focus on post-event survival rather than the precipitating event (*LOST, The Road, The Walking Dead, I am Legend*). While depictions of survival and threat in popular culture can serve as a window to imagined threats, and examining these media artifacts could work to bring governmental logics to the surface, my focus is on the subterranean spaces that represent a material investment in sustaining life in the event of crisis. These spaces—designed and built to protect and preserve life in the event of disaster—are more about *preparation for survival* than survival itself, and represent important sites in which we can understand imagined threats and post-event living.

Bunkers

> Just as the eighteenth century bastion materialized the ballistic systems of rudimentary artillery, the bunker was built in relationship to this new climate; its restrained volume, its rounded or flattened angles, the thickness its walls, the embrasure systems, the various types of concealment for its rare openings, its armor plating, iron doors, and air filters—all this depicts another military space, a new climactic reality. (Virilio, *Bunker Archeology*, 1975/1994, p. 39)

In a country where we transport the Constitution underground every night, it makes sense that we would provide underground space for people as well. For years, government involvement with disaster scenarios has entailed not only the building of public shelters, mapping of evacuation routes, and assisting in clean up from natural disasters and terrorist attacks, but also in working to ensure that in case of catastrophe, the government can continue to run, with the logic that an intact government can facilitate disaster relief, cleanup and rebuilding, and if necessary, military retaliation. This is what the FEMA Continuity of Operations Plan (COOP) provides – a flexible disaster plan that works to ensure that, in the case of a national disaster, a protocol is in place to reboot government.

The presence of underground bunker facilities should come as no surprise to many Americans, as decommissioned facilities have not only been documented, but can in fact be toured for a moderate fee and even rented out for meetings and parties. The Greenbrier Resort in White Sulphur Springs West Virginia is home to a 112,544 square foot bunker completed in 1961 that served as a backup facility for the United States Government for more than 30 years and featured an on-site power plant, water purification system, 14,000 gallon diesel storage tank, decontamination chambers, and room for more than 1,100 people (Greenbrier, 2010). Completed under the guise of adding an Exhibit Hall and two meeting rooms at the resort (which were in fact rented out to groups even as it remained a government

facility), the site featured a pharmacy, laboratory, cafeteria and meeting facilities, as well as a communication area with television production and audio recording equipment, making it a suitable location for the U.S. Government to continue operations in the event of a nuclear war. The Greenbrier website notes that the facility was exposed in an article published in *The Washington Post* in May of 1992.

A March 26, 2011 NPR story on the facility reports that the project, initially called Project Greek Island, was initiated by Dwight Eisenhower as part of a larger concern about threats in the nuclear age. Today, the facility is partially open for tours while other areas are used for data storage (NPR, 2011, para. 29). The story on the Greenbrier was inspired by reports of at least 33 complexes in Washington DC and the surrounding vicinity that have been completed or are under construction following the attacks of September 11, 2001. The articles that uncovered the facilities, written by Bill Arkin and Dana Priest, were published in the *Washington Post* through 2010. Arkin claims to know where the new backup facility is, but he is keeping that information under wraps.

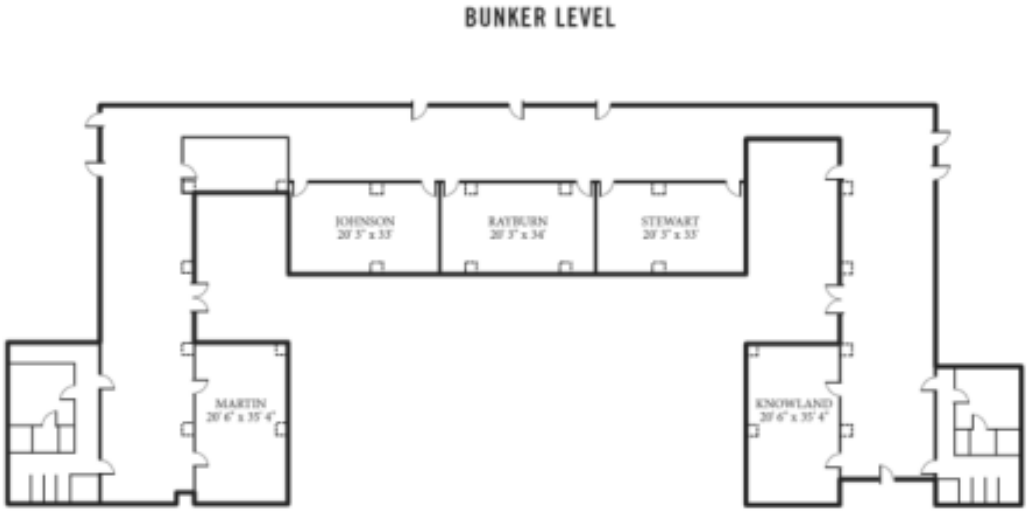

Figure 4: Greenbrier Bunker Floor Plan

The initial *Washington Post* article revealing the bunker details a long history between the U.S. Government and the resort, explaining that it was used as an internment camp for German, Italian, and Japanese diplomats during World War II and later purchased by the military as a 2,200 bed hospital, which it remained until bought back by the Chesapeake and Ohio Railroad after the war (1992, para. 10). Ted Gup explains that the facility was operated by Arlington-based company Forsythe Associates, which "has a cover that shows a genius for simplicity" in providing television repair and service at the Greenbrier (para.25). While details concerning the construction of the curious hotel wing were scarce, Gup notes that in an interview with a worker who helped to pour thousands of gallons of concrete during the construction remembered seeing "Mosler" printed on one of the giant doors installed in the facility; Mosler manufactured vault and safe doors as well as doors designed to protect against nuclear blast. While the facility was still classified at the time the article was written, Gup had it right that the largest room was hiding in plain sight: an 89 by 186 foot Exhibit Hall: "Through a vehicular entrance, exhibitors can drive truckloads of equipment and displays into the hall… A Greenbrier brochure dating from the early 1960s notes, 'The floor is finished with a beautiful plastic terrazzo designed to support unlimited weight'" (Gup, para. 39). Gup notes that two auditoriums – one seating 470 and the other 130 – would be suitable spaces for the House and Senate (para. 41). Inside, he reports beds, showers, and a dining room with "false windows complete with wooden frames and country scenes painted on them" with the idea being that "the illusion of being above ground might counter the sense of entombment that could come from a prolonged stay in the facility" (para. 45).

In the article, Gup discusses some of the issues with the Resort Bunker, including distance from Washington, D. C., challenges of mobilization, and the larger issue that the facility would not have provided room for spouses and children. He writes of walking around the Greenbrier grounds and locating one of the outside entrances:

> And it strikes me that here, before my eyes, is the very architecture of fear. The Greenbrier's secret lesson is the same one my generation learned so well: how to compartmentalize our lives. How to contain our fear just below the surface, secure and controlled -- daily denying its existence -- while above ground we manicured our lawns, concentrated on recreation and consumption, and turned up the music as loud as it would go. So too it has been with the Greenbrier. For 30 years, its guests have come to play golf, to be massaged, to bathe in the restorative waters of the mineral baths, while some of the men who repaired their televisions and brought them movies made all things ready for a darker world after this world. (para. 68)

Is the bunker under the Greenbrier indeed representative of an architecture of fear? Is that what bunkers and shelters are? Virilio (1994) examines a series of bunkers built by the German forces along the French coastline during the Second World War in *Bunker Archeology* (originally published as *Bunker Archéologie* in 1975). While these bunkers served wartime purposes of defensive positioning and storage of munitions and other military supplies, networks of fallout shelters were also established during these times in the basements of hospitals, schools, and public buildings to protect the general population.

During the Cold War in the United States, some home owners built their own family shelters in basements and backyards complete with blast doors, rations, and anti-radiation medication. While Virilio explains that “in 1943-44, everyone was advised to dig a trench in his backyard, in the courtyard, to shelter his family” (1994, p.38), he later clarifies that the experience of having lived through aerial campaigns of WWII made Europeans less likely to invest in such shelters:

> During this period [1945-1990], the myth of the anti-atomic-bomb shelter spreading like wildfire in the United States had no hold in Europe, where the memory of strategic bombing from 1943-1944 removed all credence to a policy of "passive defense." Everyone realized from experience that populations would not have enough time to get to the shelters in case of a nuclear attack. (1994, p. 200)

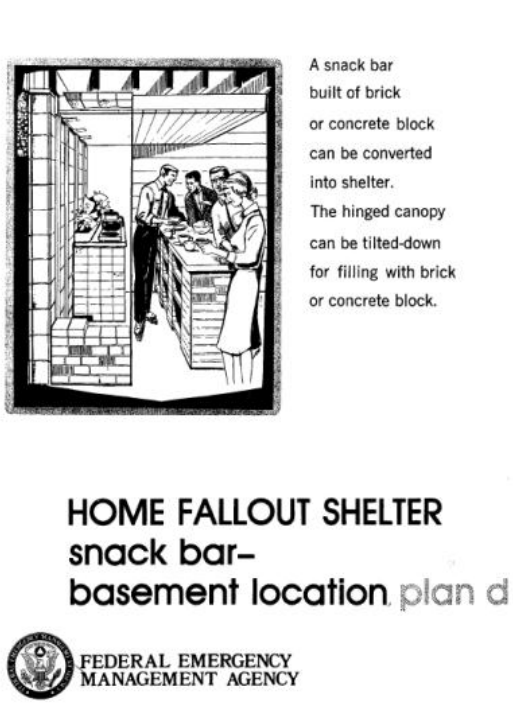

Figure 5: Home fallout shelter plans from the Federal Emergency Management Agency.

In the United States, the belief that shelters would prove effective in home defense remained strong, and the government placed the burden of safety on the citizen for quite some time, providing information that would aid the citizen in preparing for the worst. The image above, taken from an April 1980 FEMA blueprint for a "Home Fallout Shelter snack bar" (shown in Figure 5) is just one of many plans provided by the agency to aid citizens in preparing themselves. In what follows, I will examine shelter and bunker developments of the Cold War era in order to ascertain the nature of such space during a time where nuclear threats dominated a discourse of fear. After a thorough review, I will look to more recent

ideas about personal shelters, including dual-use shelters, safe rooms, community shelters, and preparations during a time when the War on Terror, 2012, and type-2 climate change have eclipsed the Red Threat and Mutually Assured Destruction of the Cold War.

As for the American People, the burden of preparation is framed as the duty of the good citizen. In their introduction to a special issue of *Cultural Studies* titled "Homeland Insecurities," Hay and Andrejevic (2006) argue that self-government is crucial in the present Homeland Security effort, and, further, that "the goal of Homeland Security becomes an alibi not just for the adoption of 'neo-liberal' economic policies, but for conducting various governmental experiments in security and mobilizing the technical resources of self-governance and personal securitization that accord with such policies" (p. 339). They argue that the strategies tied with Homeland Security are "the continuation and consolidation of multiple strategies of responsibilization, privatization, and citizen mobilization associated with the neo-liberal assault on the post-war settlement and the welfare state" and Homeland Security becomes a new locus of centralization of information and flows (p. 342). Later in the issue, Hay explores the role of citizens and the home in defense, arguing that that the current government sees security through the framework of mobile privatization, and the home as a center of civil defense. Contextualizing Department of Homeland Security efforts to mobilize citizens to secure the home in terms of a longer trajectory of suburban security including blast-proof homes, bomb shelters, and "duck and cover" campaigns, Hay points to programs that worked to encourage a strong architectural foundation for the home, promoted family and home insurance, and portrayed the securing of the home as a citizen's duty. I will address this work later in more detail, but first I will discuss ways in which Cold War Era military and government bunkers are being repurposed as spaces for civilian survival.

Rebooting the Bunker and Silo as Shelter

As the government has moved away from the provision of public shelters and instead to the neoliberal notion that the government should provide for itself through COOP planning and citizens should provide for themselves, DIY shelters continue to be built in basements, backyards, and remote areas. In recent years, however (as 2012 approaches and issues of terrorism and economic instability gain increased currency), a number of high-end community solutions are being developed. The Survival Condo is one of many private solutions for survival in the event of major crisis events in the United States (Figure 6). This particular solution also boasts a swimming pool (seen in figure 7), movie theater and hydroponics floor. In this facility, a half-floor condo is priced at $900,000 and can support three to five people, and a full floor, priced at $1.75 million, can support 6 to 10 (SurvivalCondo.com, 2011). The site notes that prices include training and a five-year food supply for each person. In addition to features that make the unit "safe," each unit includes an LED television, stainless steel kitchen appliances, washer and dryer, Kohler bath fixtures, satellite TV feeds and Internet access (SurvivalCondo.com, 2011). A page on the website titled "Cool Stuff" explains, "[i]f you are buying a 'Survival Condo' that is built from a converted Atlas 'F' Missile Base, you'd expect to have a few cool add-ons and gadgets" and goes on to list features such as 50KW wind turbine, guns and ammunition, and a military grade thermal imaging security system.

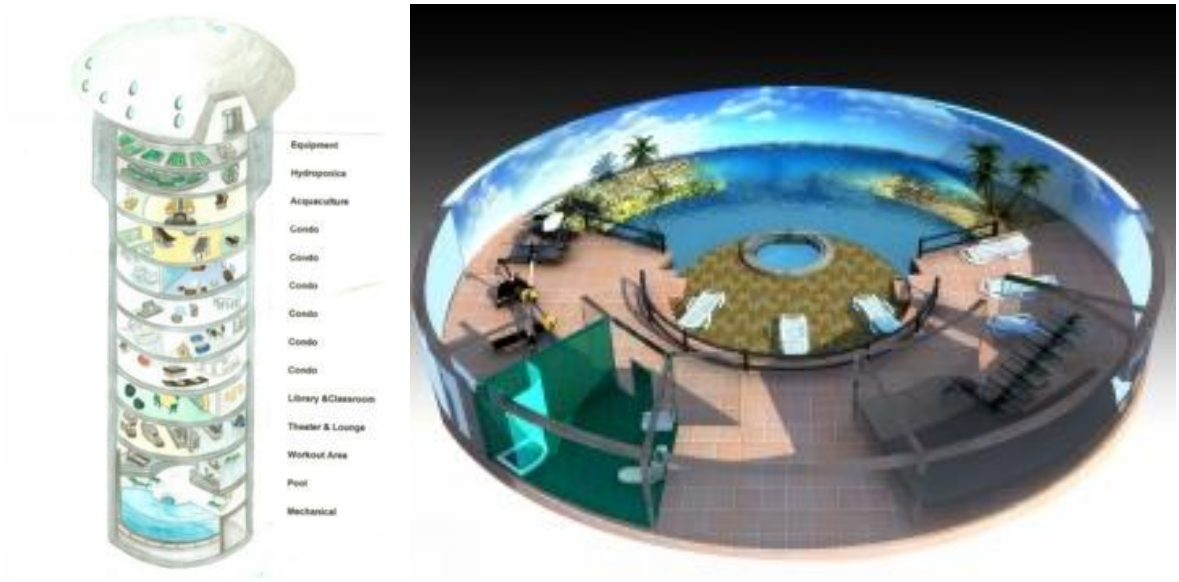

Figure 6: (left) Survival Condo concept.
Figure 7: (right) Survival Condo pool-level amenities.

The builder explains that using already constructed facilities gave them a "$60 million dollar head start" and that these structures are some of the strongest built of all time. Images of the original construction in the 1960s are available on the site and provide a certain sense of safety, as a potential buyer can see the amount of labor, rebar, and concrete that went into the original project. These images work to reassure visitors to the site that the facility is strong enough to withstand the range of threats listed on the site, which include: climate change (with sub-sections discussing hurricanes, tornados, earthquakes, drought, floods, hot spots, volcanic ash and volcanoes), pole shift, Planet X, solar storms, galactic plane, alien contact, civil unrest, terrorism, pandemic, and 2012.

If sharing a converted silo with more than 50 people is not your style, finished silo homes are also available for purchase from 20th Century Castles, LLC, a company which helps to facilitate the sale of abandoned and refurbished bunker facilities and bunker homes. One such home—built on the site of an Atlas F missile base in New York's Adirondack State

Park—boasts an FAA approved runway, 2,000 square foot surface home, a new well and original septic tank (Figure 8). In addition to a finished launch control room with three bedrooms and two and a half baths, "[h]uge doors open to a large tunnel that accesses the silo that has an additional 20,000 square feet of useable space with unlimited possibilities. The perfect getaway home, it has its own direct runway access, it is climate controlled and is capable of withstanding a nuclear hit" (20th Century Castles LLC, 2011). While this home is listed for sale at $4.6 million U.S.D., more affordable sites include a number of communications vaults and bunkers in the $300K range.

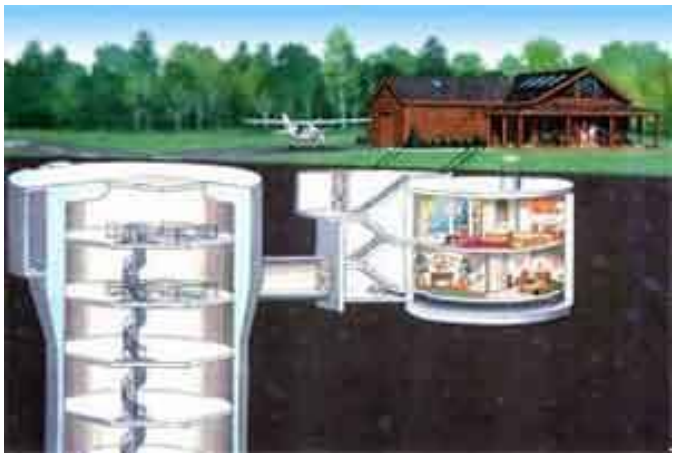

Figure 8: Atlas F missile base, Adirondack Mountains, NY.

Vivos, described on their website as a "life assurance solution," constitutes a new way of thinking about civilian spaces of survival. A video on the site landing page opens with white text on a black screen: "Many people believe we are living in the end times" and after a slow motion shot of a group of anonymous people walking on what could be any city street: "What if the prophesies are true?" (Vivos Group, 2011). Showing a computer generated sequence of an asteroid approaching Earth, the video asks, "Do you have a survival solution for your family?" and cuts back to the asteroid entering the atmosphere and striking

the surface as text reads: “Time may be running out. The risks are all around us,” before moving through a series of icons representing threats that are later featured on their web page such as nuclear war, terrorism, anarchy, killer comet, pole shift, global tsunami and Planet X (an undiscovered planet that some believe could interfere with our solar system in numerous ways, including pole shift, comet collision, and extreme weather events).

The video then asks “What has the government been preparing for? Will there be another life extinction event?” before showing rendered images of the inside of the shelter and stating that “VIVOS is building a network of shelters. To survive whatever may be coming our way.” The rendered animation of half the Earth in flames suggests a seriously apocalyptic scenario, while an image of a personal dorm area in the shelter offers sanctuary. “Where would you go with 3 days’ notice?” the text asks, before showing a doomsday clock centered on the year 2012. “The ultimate life assurance solution,” the text reads, before the following images are displayed: a mushroom cloud, a blue human eye with long eyelashes, a woman holding a baby, an older woman with two men wearing suits in the background, a middle-aged man and woman sitting outside, and a man and two children on the beach (the older child with his head in his hands) before flashing back to the company logo, another image of the shelter, and finally the site address. (All people in the video are Caucasian.)

Once a visitor enters the website, the doomsday clock featured in the video serves as a hub for one set of links on the site, and the icons denoting the various risks are another set of links that examine the scenarios that the shelter is designed to withstand. I call it a doomsday clock because there is a counter below it showing—down to the second— time remaining until to December 21, 2012. A last set of links include one to apply for space as well as news, contact information, and even a “gear” links to a page featuring a range of

survival necessities: “our experts have done the analysis and shopping for you, selecting the ultimate gear from each of these sources, to enhance your chances of survival from whatever threats you may encounter” (Vivos Group, Survival Gear, 2011).

In addition to information on newly constructed survival communities, the site features information on a 137,000-square-foot Nebraska facility (Figure 9) in which Vivos is currently offering 900 spaces at $25,000 per person. The site explains that the low price of co-ownership in this facility lies in the economy of scale provided by the shelter, located within a day’s driving distance of anywhere in the United States. In a document explaining some of the features of the Nebraska site, the Vivos Group explains that while the site is in a rural area with food and water resources, it is also “In the ‘safe land zones’ envisioned on many futurist maps” and located only 70 miles from Omaha, the “probable alternate capitol of the U.S. should Washington D.C. become compromised” (2011, Nebraska Features).

According to the Vivos website, the features of the facility itself include semi-private bedrooms and bathrooms, a year of supplies, and a community kitchen. Features that one might be less likely to expect include a fully stocked wine cellar, a full wardrobe, classroom, theater, hair salon, and CCTV and radio communication center. Defensive features include a 10-mile defense lookout, remote sensing devices, and, within the shelter, a vault, a “security and detention center” and storage area for ATVs and armored vehicles. There is also space for non-hybrid seed and DNA storage. Unlike the rendered images which represent plans for original construction, the Nebraska facility appears to have been converted from an existing shelter, possibly an abandoned government bunker facility. Floor plans for this shelter represent the solution in existing space, which is what has enabled these spaces to be offered at half of normal cost.

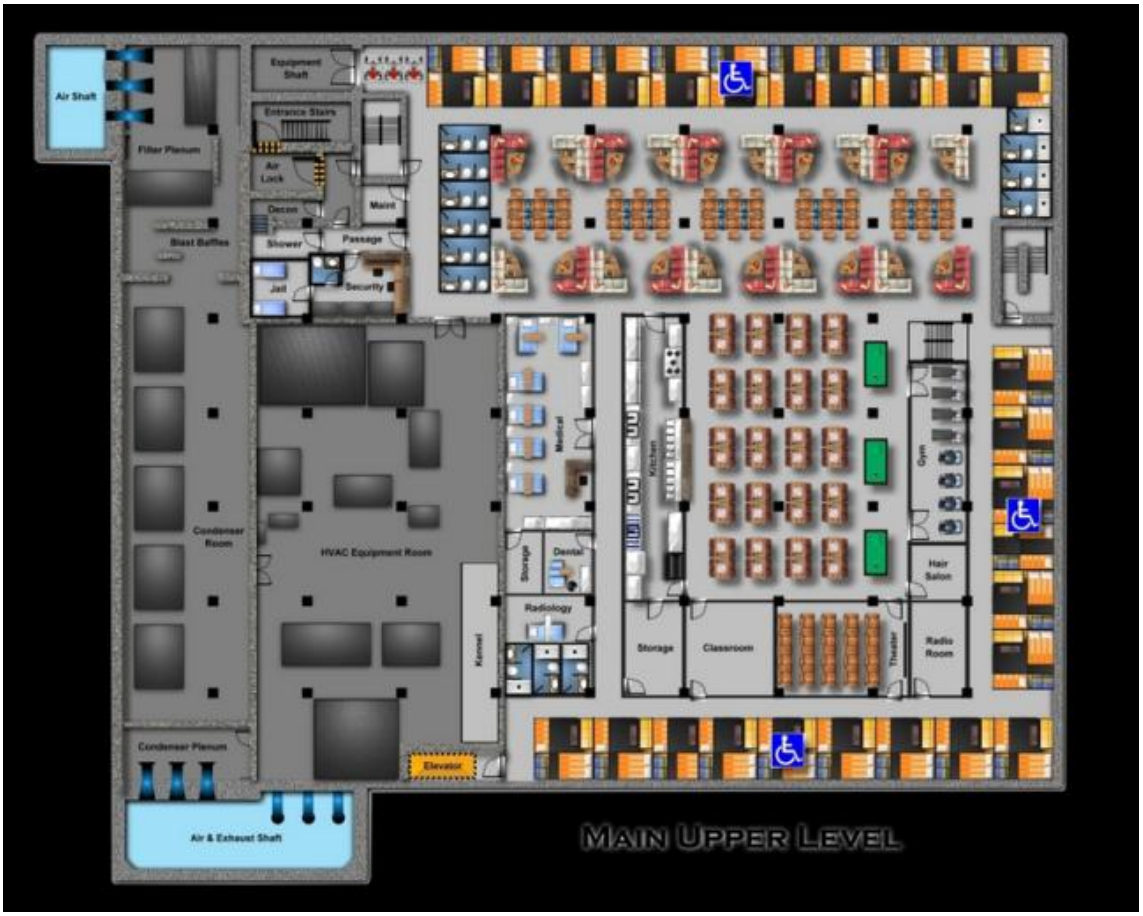

Figure 9: Main Upper Level of the Vivos four-level Nebraska Facility.

With the Greenbrier facility declassified and so many former bunker, communication, and missile silo sites becoming re-worked as spaces of citizen survival, one has to imagine that new spaces for underground governance exist. Of course, we do not know where they are, what they look like, and what they are designed to withstand. What can be analyzed is publicly available marketing information and plans for newly imagined spaces of community survival, which will illuminate new imaginaries of survival and survivorship in a society dominated by the interconnected and (nearly) always-available grid.

From Underground Up – The Production of Shelter Space

While various refits of pre-existing structures as discussed above (such as the Nebraska facility) provide examples of the ways in which old spaces are being made to serve new purposes, their examination alone is not sufficient. The Nebraska Facility, like others built from former military bases and missile silos, represents a re-working of the same "architecture of fear" that Gup described as he revealed the bunker facility at the Greenbrier. While it would be as worthy an effort to look at how military spaces have been re-represented or re-booted as spaces for the continuance of civilian life, I argue that if we are to truly understand how these spaces are presently imagined to serve as protection from threat and survival in times of extended immobility, we must look to new construction: new productions of survival space. For this reason, I have chosen to analyze the original concepts for the solution as a space created from scratch to secure against threat in the present.

One route to understanding the ways in which disconnection from the grid operates is in looking at the design of spaces produced for the sole purpose of protecting individuals from danger in the event of disaster or attack. Such spaces constitute an actualization of a set of logics dealing with survival and life after the grid. Wiley (2005) explains that "[a]ctualization is the process whereby a virtual multiplicity is incarnated in an actual body with extension or corporeality" which "can also be understood as a concrete solution to a virtual 'problem'— an organization of substance in a limited space and time that achieves a particular purpose" (p. 70). Here, the shelters created by the Vivos Group will be examined as one such corporeal body, or actualization of a set of logics that deal with the place of infrastructure in ensuring survival in uncertain times in an "ongoing production of the real" that occurs in space through the production of space (Wiley, 2005, p. 70). What Deleuze and

Guattari term “concrete assemblages,” also understood as those actualities, are *effectuated* or produced by abstract machines, those logics which establish relations between elements. In order to work toward an understanding of logics effectuated in the Vivos shelter and other shelter solutions, I analyze the production of such spaces in a spatial materialist tradition that has its roots in the work of Deleuze and Guattari (1987) and Henri Lefebvre (1991), and has been taken up by communication and geography scholars including Hay (2001; 2003; 2008), Couldry and McCarthy (2004), Jansson and Falkheimer (2006) and Soja (1999).

In "Locating the televisual" (2001), James Hay suggests that viewing the televisual “as a sociospatial problematic” is a way of considering the role of "social bodies (individuals and populations) in terms of mobility and access to and from the sites where TV is located” (2001, p. 215). Following Lefebvre, Hay understands space as both produced and productive, and suggests Williams’ notion of mobile privatization as a potential starting point for such a project, as it "concerns a new spatial distribution and arrangement of social subjects" where "[t]elevision, as cultural technology, becomes a necessary technique for living within this social arrangement and material environment” (2001, p. 218). In a 2006 article, Hay explores the role of citizens and the home in defense, arguing that that the current government rationality sees security in the framework of mobile privatization, with the home constituting a center of civil defense. In this piece, Hay contextualizes Department of Homeland Security efforts to mobilize citizens to secure the home by placing those efforts in a longer trajectory of suburban security that includes the blast-proof homes, bomb shelters, and “duck and cover” campaigns of the 50s and 60s. Using Williams’ mobile privatization as “a way of thinking about current forms of mobilization around safety and security that have occurred within a current regime of mobility and privacy” (Hay, 2003, p. 355), he identifies programs

that worked toward a strong architectural foundation for the home, promoted family and home insurance, and positioned securing the home as a citizen's duty. In focusing on the place of the home in such discourses, Hay's analysis takes issues of the materiality of space as a central component to understanding larger shifts in thinking about personal and family safety, national security, and shelter as media. As Virilio argued in *Bunker Archeology* (1975/1994), Hay's work suggests that the home, like the bunker, serves a particular time and purpose in the same way that clothing does. Virilio explains that the terms used for clothing and those used to describe the other coverings, indicate that:

> The fortification is a special construction; one does not live there, one executes particular actions there, at a particular moment, during conflict or in a troubled period. Just as you put on your armor for combat, your raincoat in the rain, you go to the fort when the peacetime conditions of the environment yield to wartime weather conditions. (1994, p.42)

Hay argues elsewhere that media must be thought not only in such spatial and material terms, but conceived more broadly, arguing in a 2008 article that: "'the long history of new media' is just as much a history produced by and through space, transport, travel, mobility, houses, cars, trains, clothes, and refrigerators as it is a history of communication 'media' and their industries and cultures" (p. 67). In this regard, an examination of survival solutions takes the material spaces of survival in an informational economy as a central site for understanding culture, mobility, threat and survival in informational society.

In the introduction to their edited collection *MediaSpace* (2004), Couldry & McCarthy argue that "it is ever more difficult to tell a story of social space without also telling a story of media, and vice versa" (p. 1). Drawing attention to the importance of focusing on the material spaces of communication, they identify five levels of mediaspace: 1) media representations; 2) the flow of media across space and the ways that media reconfigure

social space; 3) spaces of production and consumption; 4) scale-effects caused by media in space; and 5) experience and understanding of media-induced entanglements of scale (p. 5-8). In looking to the Vivos Group's solution, we might understand this analysis as addressing a number of those levels, including a focus on representations of the shelter, the ways that informationalization has affected shelter space, and the change in scale of shelters as network communities rather than family-scale shelters brought on by an increased awareness of network value driven by larger social networking discourses.

Calling for a spatial turn in media studies, Jansson and Falkhiemer (2006) argue that informational society is operating under a regime of "hyper-space-biased communication" which embodies "spatial ambiguities" such as increased mobility of people and technologies, technological and cultural convergence, and a dilemma of interactivity between sites of production and sites of consumption (pp. 11- 13). They argue that this spatial turn in media studies would overcome the ephemerality of texts, contexts, and text-context relationships through an analysis that considers: 1) an ideological and political dimension that influence the production of space; 2) a technological dimension that looks at how technologies shape and are shaped by communication processes; and 3) a textural dimension that looks at how space is materialized through culture. Jansson further explains this concept of "texture" as the stuff that both holds together and alters space, presenting a method of textural analysis that would explore the "intersections of symbolic and material geographies of communication, as well as the ideological embeddedness of communicative practices and technologies" (p. 87). Jansson's framework suggests focusing on media spaces as actively produced in the sense of Lefebvre's spatial triad of lived, conceived and perceived at the local, institutional and global scales as a starting point for understanding the ways that changes in communication systems

become incorporated with or change systems. This concept is not so different from Soja's argument that a "critical thirding" that reincorporates space with history and sociality is central to enriching critical inquiry.

In *Thirdspace* (1999), Soja focuses on the work of geographer Henri Lefebvre, redescribing his triad in terms of: 1) spatial practice as firstspace, which is material space; 2) representations of space as secondspace, the space of signs and ideology; and 3) thirdspace, resonating with Lefebvre's representational space (or as Soja re-translates, "spaces of representation"), which he describes as combining elements of firstspace and secondspace while moving beyond both in a process of "thirding." While Lefebvre describes spaces of representation as directly lived by inhabitants, users, artists and "a few writers and philosophers, who describe and aspire to do no more than describe" space (p. 39), Soja's Thirdspace is:

> …a knowable and unknowable, real and imagined lifeworld of experiences, emotions, events, and political choices that is existentially shaped by the generative and problematic interplay between centers and peripheries, the abstract and concrete, the impassioned spaces of the conceptual and the lived, marked out materially and metaphorically in spatial praxis, the transformation of (spatial) knowledge into (spatial) action in a field of unevenly developed (spatial) power. (p. 31)

Lefebvre's spatial triad in *The Production of Space* can be used as a framework through which to understand the production of the survival space. In *The Production of Space* (1991), Lefebvre works toward an analysis that would prove that a "science of space" represents the political use of knowledge in production and social relations, conceals this use through ideology "indistinguishable from knowledge," and "embodies at best a technological utopia… a common feature not just of many science-fiction novels, but also of all kinds of projects concerned with space, be they those of architecture, urbanism or social planning"

(pp. 8-9). Space, for Lefebvre, is an active site that must be examined, questioned, and understood. Along these lines, the spatial triad can be seen as a framework for understanding what Lefebvre sees as three fundamental elements of space, which taken together represent a knowledge of space: spatial practice (perceived space), representations of space (conceived space), and representational spaces (lived space). In this analysis, I work towards an understanding of the ways in which communication has become central to the infrastructures and design of the shelter through an examination of shelter space using the elements of the spatial triad to gain knowledge of such spaces, beginning by asking a few questions such as:

- From what are individuals seeking shelter?
- What role does the individual play in producing or customizing this space?
- What do shelters serve as protection from?
- What flows enter and exit this space?
- What does the Vivos solution tell us about imaginaries of life after disaster?

Perceived space is also known through spatial practices, which are "revealed through the deciphering of" society's space (Lefebvre, 1991, p. 38). Examining the way that spaces are perceived can be done through careful observation of uses of that space which "ensures continuity and some degree of cohesion" and "implies a guaranteed level of *competence* and a specific level of *performance*" (p. 33). At present, spatial practices of these particular communities cannot be observed, as the locations of sites are secret, their members anonymous, and in many cases, yet to be constructed. What can be observed is conceived space, or what Soja refers to as firstspace (material space). Here I will look to the material concerns, such as where shelters are located, what they are constructed from, what they can endure, and their capacities in terms of bodies and supplies.

First and foremost, the Vivos Group advertises their solution not as one centrally located shelter, but as a network of shelters consisting of 20 across North America, four in

Europe, and anywhere else in the world where at least 200 members are. While the sites are kept private, all sites are located within a safe distance from potential targets and at higher altitudes for water runoff in the event of flood or mega tsunami. A main catchphrase on the site, "Where would you go with 3 days notice?" asks users to think in a different timeframe for getting to a safe space to ride out a potential crisis. With a shelter within a day's drive of virtually anywhere in the U.S., the site reminds visitors through whitepapers, video clips, and specific pages for a number of threats that there is enough advance notice with most catastrophic life threatening events (such as a coming meteor) that travelling to a secure shelter is preferable to going it alone in a backyard bunker which does not provide the same levels of security as a community shelter. Working to dispel the notion that a person should be able to get to their shelter in 20 minutes, they explain that this time frame assumes that a subject is at home and ready to enter and seal the shelter, which they argue is not practical.

In a section of the site titled "Will You Survive In A Backyard Shelter?" the company addresses a number of common questions about the difference between the backyard shelter, which an individual can build or have constructed on their own property or at a nearby location to support themselves and their family for a number of days in the event of a crisis. One of the first concerns that the page addresses is the sheer difference in the quality of materials used in a backyard shelter and the high-quality materials used to construct a their community shelters. The second is perhaps more troubling for the suburban citizen: in a time of crisis, how will you defend your shelter, even from your own neighbor? The construction alone may raise eyebrows, nosy neighbors pry, and permitting provides the paper trail for snoopers. The site warns that "When the time comes, you will need to fight off your 'friends', neighbors and even relatives, all wanting access [sic] from a pending catastrophe,

or worse yet, trying to break in after you've sealed the door" (2011, para. 6). By contrast, Vivos shelter locations are kept confidential, but in the case that the local population knows of the shelter (as was the case with many residents in White Sulphur Springs where the Greenbrier facility was located), facilities are "equipped with high-security barriers, fencing, devices and a security team that is ready, willing and very able to defend their complex… Unfortunately, a backyard home shelter does not include these security measures that are absolutely necessary for the ongoing integrity and success of any shelter" (para. 6). The claim to superior security is further supported by the answer to the next question the document answers regarding the number of well trained and armed persons in each community: "approximately one-third of all Vivos Members have Military and/or Law Enforcement backgrounds" which, combined with the other assets of the facility do far more to protect than would a backyard bunker. In other words: there will be guns. Lots of guns.

The concept, according to the site, "is based on a spoke cluster of 10 radiating residential wings, surrounding a 2 story, 60 foot diameter central dome. The complex includes community gathering areas and private suites providing comfortable and spacious accommodations with about 100 square feet per person" (Vivos Group, 2011). Each shelter "community" will be capable of accommodating up to 1,000 people for one years' time, stocked with the necessary food, clothing, and medical supplies for the population inside. These facilities are specifically designed to be self-sustainable in the event of a multitude of scenarios and contain what constitutes a micro grid of services including electrical power, water, sewage disposal, and air filtration. In addition to these "private works" infrastructures, the facilities will also be equipped with security devices and contain hunting and fishing supplies as well as off-road vehicles for when the surface is safe again. According to the

portion of the website dealing with the security of the shelter design, the company lists a range of forces of potential disasters the shelters can withstand:

- Force 10 magnitude earthquakes in succession
- 450 MPH surface winds
- 50 megaton air burst detonated 10 miles away
- Solar flares in excess of 1,000,000 volts
- Flooding submersion
- Extreme external fires at 1,250 Fahrenheit
- Magnetic pole shift
- Radiological, chemical and biological weapons
- Excessive accumulations of snow and rain
- A fortress in the event of social anarchy
  (Vivos Group, Threat Scenarios, 2011)

In addition to these safety features, the shelters include amenities such as meeting areas, AV equipment and a communications center, exercise area, a vault for valuables, and a salon. Spaces included invoke a particular kind of order and way of life in the bunker, and next I look to the conceptualizations for life inside as they are suggested by the internal design of the facilities.

Figure 10: Gallery of Vivos shelter images.

Representations of space, also called conceived space by Lefebvre, are "tied to the relations of production and to the 'order' which those relations impose, and hence to knowledge, to signs, to codes" (1991, p. 38). Lefebvre also refers to this as "conceptualized space," it is the space of "scientists, planners, urbanists, technocratic subdividers and social engineers, as of a certain type of artist with a scientific bent" as opposed to the representational or lived space of users (1991, p. 38). In terms of this analysis, we will understand this space along the lines of Soja's secondspace, the space of signs and ideology. Here I will examine in more detail the inclusion of specific institutional spaces in the shelter that demonstrate a particular understanding of "order" and "society," such as the detention center, the medical area, the classroom and the beauty salon. In this way, I will demonstrate that these shelters are designed with a particular conception of what "society" should look like underground in addition to reflecting present-day values above ground, and examine the ways in which these and other amenities suggest a particular social order.

In my research on the Vivos website, one question in a Q&A that compared the benefits of the Vivos solution with that of the backyard bunker was particularly informative as to the way in which the designers viewed the space as being instrumental to long term underground survival:

> Underground survival takes extreme tolls on the human body, mind and spirit. You will not survive in something hardly bigger than a small shipping container, without space to move around, and a community of talented people with various backgrounds and expertise (physicians, laborers, artists, security, survivalists, etc.) to help you get through all of the physical and mental challenges. Being in a community of like-minded people with an abundance of supplies, amenities and 'creature comforts' is essential for your survival as well as your sanity. This type of diversified preparedness co-ownership shelter community, with ample space per person to exercise, move around, find privacy, and/or gather socially, is only currently available through Vivos. (Vivos Group, 2011)

My goal here is not to argue that this solution indicates a disciplinary form of power, but to not mention the following would seem careless: featured in a central location in the facility are a detention center, classroom, and medical area. Clearly, confinement is going to be a factor in an environment designed to seal a group off from the outside world. What I am interested in here is the ways that the organization of space and the actions of the Vivos organization work to help establish governance in these spaces. The site explains:

> Prior to any engagement of a Vivos shelter, the Vivos Group will provide operational oversight of each Owners' Association for ongoing maintenance, replenishment, security, monitoring, surveillance, notifications and advisories. Once a facility is occupied and under lock down, the co-owners will elect a board and takeover autonomous operation and management of their Vivos facility. (Vivos Group, 2011)

With this, it is apparent that the organization anticipates a need to set up a government once the facility is secure from external harm. The value of governance, taken with the layout of the structure itself, begins to get at a sense of thirdspace, that "lifeworld of experiences" both real and imagined, knowable and unknowable, and at the intersection of spatial knowledge, action, and, ultimately, power (Soja, 1999). In the shelter, lived space is secured from an imagined future both unknowable and dangerous through the capacities of the material aspects of the structure and within though the ordering of space. Asking site visitors to imagine future scenarios both from the perspective of an ordinary person and then as a co-owner is a particularly important function of the Vivos web site, particularly through the lens of a variety of the scenarios that the site suggests: nuclear war, bio war, terrorism, anarchy, electro-magnetic pulse, solar flares, pole shift, killer comet, global tsunami, Planet X, and supervolcano. While describing threat scenarios in detail would distract from the focus of this chapter, each suggests that coownership in a Vivos facility is a smart alternative to no shelter, backyard and basement shelters, or waiting for government support or assistance. It is not

enough to create a space capable of housing, feeding, and supplying survivors, however: community shelter solutions also rely on the production of a "smart subject." Next, I will demonstrate the way in which this subject works to support a "grid away from the grid" solution through a particular mode of caring for the self that positions survival as a moral good, and that not only works within, but supports logics of neoliberal governmentality. I begin by discussing the process through which members are selected before discussing what the smart subject looks like in terms of the "survivor" versus "survivalist" dichotomy.

The "Survivor" as Smart Subject

> Defensive architecture is therefore instrumental, existing less in itself than with a view to "doing" something: waiting, watching, then acting or, rather, reacting. To live in such a place is not so much to "dwell" there as it is to "take it on" for an act for which the casemate is the instrument. (Virilio, 1975/1994, p. 43)

In order to secure space in a Vivos facility, potential co-owners must first fill out an application form that an anonymous selection committee reviews to determine candidacy for membership. The first area of the form – "personal information"—asks for first and last name, age, address and phone number and email as well as an optional box to identify who referred you to the site, if anyone, and then asks how the applicant heard about Vivos, with a drop down box providing a range of selections: [blank], search engine, radio, newspaper, magazine, television, referred by a friend, blog, twitter, facebook, and other. The next section of the form is titled "Skills & Expertise" and the instructions read: "Check each professional area/field that you have expertise in, or a good working knowledge of" (Vivos Membership Application, 2011). The list consists of 51 check boxes that include industry specialties and skills including physician, scientist, beautician, survivalist, automotive, seamstress, artist, fireman, martial artist, veterinarian, educator, fisherman, lawyer, law enforcement and

religion. The next section is "Comments," and consists of an open response area where users are asked to describe why they would be a benefit to the community, and the final section of page 1 is "Correspondence" where users can select where they would like official documents and newsletters to be mailed, and are also asked to create a password for their account. The second page of the application cannot be accessed until page one has been filled out[4].

After applications have been reviewed, the site explains, the organization selects candidates for co-ownership for shelters from the pool of members. Selected candidates are then offered co-ownership and a reservation agreement for a shelter located "closest to their home area" (Vivos Group, 2011). Once a certain number are collected for a given shelter, owners purchase their interest and an escrow is opened to fund construction. A note on the site explains that as of April 15, 2011, prices will be based on the gold standard at $50,000 per person or the cost to purchase 36 ounces of gold. Shelters currently costing $25,000 per person, such as the Nebraska site, will cost the purchase price of 10 ounces of gold (Vivos Group, Gold Standard, 2011). Prices are locked in at time of reservation.

A whitepaper on the site –"Surviving Economic Anarchy"—explains that of the many threats that the shelters are designed to withstand, "[m]any financial experts believe our greatest near term risk is that of social anarchy, brought on by an economic collapse, or an attack on our infrastructure" (Vivos Group, 2009). Using the 1992 L.A. Riots as an example, the paper argues that lawlessness follows interruption of services, and that the government will be unable to provide for the general population. In what sounds much like the zombie apocalypse, the paper goes on to say: "…there will be hunger, sickness, death, and destruction everywhere you turn…. gangs, thieves, or even ad-hoc militias, one way or

[4] It is unclear whether information collected is part of an actual screening process, a marketing ploy, or both.

another you will find yourself in a situation that requires years of experience and training in the proper countermeasures to stay alive" (p. 1). Further, the home is not a suitable space, as the home becomes a target and "[e]ven a small light in the dark will be a sign of your whereabouts and a signal that you have something – electricity, batteries, or fuel. Sooner or later, the 'have not's' will arrive to take it" (p. 1). The paper explains that the likely alternative of building a remote shelter that could sustain life for more than a year is similarly dangerous, as though these shelters may be hard to find and access, eventually you would be found and your supplies and safety would be compromised. Without an arsenal, combat training, and extreme survival skills, they warn, this DIY survival is not a tenable solution.

> An alternative, commercial solution is to join Vivos and have a turnkey shelter fully stocked and equipped for up to one year of underground survival… Collectively this Vivos community will be able to provide each other with security and defense, medical, survival education, cooking, hunting, farming and virtually every skill and service that will be needed to survive a long term need for shelter. (2009, p. 2)

Interestingly, throughout the site the subject position of "survivor" is contrasted with "survivalist" in important ways, including a white paper explaining the difference between the two modes of being: "Survivalist Versus Survivors: Vivos is not about 'survivalist,' but rather surviving" (Vivos Group, 2010). The document explains that while a survivalist is "a person who makes preparations to survive a widespread catastrophe, as an atomic war or anarchy, esp. by storing food and weapons," a survivor is "a person that survives… who continues to function or prosper in spite of opposition, hardship, or setbacks" (p. 1). While training to be a survivalist takes years, "Vivos members do not need to spend years studying and preparing. They only need to show up at a Vivos facility where everything needed is ready and waiting – complete and abundant enough for up to one year of autonomous,

underground survival from virtually any threat nature or mankind can create" (p. 1). Survivalists can be survivors, but survivors do not need to be survivalists—just members.

The document explains that survivalism picked up again post-9/11 and outlines a number of "survivalist scenarios and outlooks" including safety preparedness, wilderness survival, self-defense, natural disaster (brief, years long, indefinite), bio-chemical, Malthusian (population crash), Biblical, Rawlesian, and medical crisis oriented. The document also notes that while survivalism is often associated with paramilitary activity and extremism in popular culture, "Vivos is a turnkey commercial solution for everyone… the community solution for the masses… you will only need to get there. Everything else is provided, including food, water, fuel, clothing, medical supplies, communications devices, security measures, as well as extremely comfortable accommodations" (p. 4). So unlike survivalism, if anything is going to be extreme in the Vivos shelter, it is going to be how comfortable the accommodations are.

Another section of the site—"Chosen"— explains that "[h]istory has demonstrated that the masses do not take action to prepare, or even to react with self direction in the face of imminent danger" linking to a page that lists the four stages of "preparedness denial." Here, the site explains, "Survivors act on their own and take the security of their life into their own hands… These individuals that take control of their own destiny may very well be the proverbial 'chosen few,' who have made the personal choice to heed the warnings and prepare for themselves and their families, versus becoming victims" (Vivos Group, 2011, para 1). Asking "Are you a survivor?" a link points to a clip from *The Glenn Beck Show* where host Beck interviews Ben Sherwood, author of *The Survivors Club* (2009), founder and CEO of The Survivors Club ™, and president of ABC News. In the segment, Sherwood

explains the 10/80/10 rule, which describes how populations have historically behaved during the crisis. Ten percent behave in negative and self-destructive ways, while 80 percent fall into "behavioral inaction," doing nothing until told what to do by an authority figure. A final ten percent, Sherwood explains, are leaders who are "the ones, when a crisis happens, who respond decisively, purposefully, they know what to do, they've got a plan, and they take action, and they often save a lot of those people in the 80 percent who are milling around trying to figure out what to do" (Sherwood, interviewed on the Glenn Beck Show, February 20, 2009). The most important thing, Sherwood explains, is to be prepared in advance for crisis so that "you've actually already thought about it, you've rehearsed in your mind what you want to do, so that you can take that action" (Sherwood, 2009). Much of surviving, he explains, deals with anticipating the worst, and more than just having a plan, "survival is a mindset—it's a way of seeing the world."

Vivos features this clip on their site in order to further define what is meant by being a "survivor." Interestingly, the interview with Sherwood does more to demonstrate that the Vivos solution is advocating for a particular mode of subjectivity that places particular emphasis on being a survivor as a moral subject position. In his interview with Rabinow and Dreyfus, "On the genealogy of ethics: an Overview of a work in progress," Foucault explains that ethics, or "how the individual is supposed to constitute himself as a moral subject" is composed of four major aspects: ethical substance (*substance ethique*), the mode of subjectivation (*mode d'assujettissement*), self-forming activity (*pratique de soi*/ *l'ascetisme* — *asceticism*), and telos (*teleologie*) (2003, p. 111-112). In coming to an understanding of the ways in which the "survivor" represents an important ethical subject position in terms of caring not only for the self, but for "the other 80 percent" of the population without direction

or purpose in a post-even scenario. The production and maintenance of this form of self care will be explored in terms of its ethical dimension of caring for the self as caring for others, leveraging commercial solutions or "being in the know" rather than knowledge, and a revival of the Stoic traditions of *khrēsis* (the use of objects, attitudes and relationships) and *askesis* (testing preparedness) rather than repentance and self-disclosure which replaced these practices in the Christian Era (Foucault, 2005).

By looking at the operations that a member performs in order to become and continue to be a member, it is my intention to arrive at an understanding of what it means to be a survivor in terms of being a co-owner. Through Foucault's technologies of the self, it is my hope to explore purchasing an interest in a community shelter as a technology of the self akin to the techniques of self care and self renunciation of the Greeks and Christians, respectively. First, I will set the context for this development by presenting Foucault's discussion of technologies of the self, and then I will discuss the how investing in survival is posed as an ethical alternative to survivalism, chaos, and non-direction.

Foucault claims that his goal for more than a quarter of a century was to illustrate the ways that humans "develop knowledge about themselves" and to analyze the sciences as "very specific 'truth games' related to specific techniques that human beings use to understand themselves" (2003, p. 146). Stating that there are four main technologies, those of production, sign systems, power, and the self, he explains that the technologies of power and the self have mostly kept his attention, and is interested in "the interaction between oneself and others, and in the technologies of individual domination, in the mode of action that an individual exercises upon himself by means of technologies of the self" (2003, p. 147). The technologies of the self are explained as those which "permit the individuals to effect by their

own means, or with the help of others, a certain number of operations on their own bodies and souls, thoughts, conduct, and way of being, so as to transform themselves in order to attain a certain state of happiness, purity, wisdom, perfection, or immortality" (p. 146).

Foucault discusses Stoic techniques of the self, including askesis, which entails progressive consideration and mastery over one's self with the final aim of understanding the world. It consists of exercises where the subject puts himself into a situation (imagined or real) to test his preparedness, much like the site asks users to do as they click on various icons that link to pages that describe a range of potential scenarios. Examining the transition from pagan to Christian culture to identify continuities and discontinuities, Foucault explains that in Christianity, techniques of the self are largely a truth game. Christianity imposes truth obligations more strict than the preceding pagan religions; truth in faith and self are linked together, making a purification of the soul impossible without self-knowledge (Foucault, 2003). This truth/faith connection can be seen in two major practices of early Christianity: recognition and penitence. Recognition consisted of the disclosure of the self dependent on a "recognition of fact," where Christians identified themselves as such publicly, while penitence went a step further, requiring not only a recognition of one's status as a sinner but self-discovery and purification of self through punishment, suffering, and shame. Identification of oneself as a survivor among a community of survivors achieves a form of recognition while at the same time providing a "chosen" status that excludes survivors from the penitence that others will pay for their inability to prepare. Foucault argues that the correlation between techniques of disclosure of the self in Christianity (both dramatic and verbalized) and the renunciation of the self are important, though verbalization takes on great importance from the eighteenth century on. The use of these techniques of verbalization in

the human sciences, he argues, "to constitute, positively, a new self… without renouncing oneself constitutes a decisive break" (2003, p. 167). The subject position "survivor" does exactly this: it enables the creation of a new "surviving" self that does not need to renounce the existing neoliberal subject in the way that a "survivalist" self does. Purchasing an option in a community shelter is a way to ensure that you will be among the chosen (a subject who has made the moral decision to be among the leading class in a post-event society) without renouncing the comforts of everyday life (like going to church at Christmas and Easter but staying home to watch the game every other Sunday of the year). This can be better understood by looking at "ethical substance," which Foucault describes in other late work.

In the working sessions with Rabinow and Dreyfus, Foucault (2003) explains that ethical substance—the aspect of the self or behavior occupied with the concern for moral conduct—is "not always the same part of ourselves, or of our behavior, which is relevant for ethical judgment," and changes depending on the field of morality that one is operating in (p. 111). In imagining a much changed field of operations, the survival scenarios listed on the site demonstrate a range of potential futures in which a subject may be required to operate: the site poses survival itself, and particularly the ability to lead others through uncertain situations, as a moral obligation (not too different than the logic that legitimates COOP: the government must also survive to look after the flock subjects who survive). The ethical substance, then, or the part of the self occupied with moral conduct, is the survivor: one who does not practice survivalism or engage in paramilitary activities, but an everyday person who is willing to switch gears and lead, or survive, on a moment's notice.[5]

[5] The majority of the shelter options discussed here (as well as the backyard shelter option) require a substantial monetary investment and a minimal time investment, whereas survivalism is the inverse (much time for training is required, but little money). The subject position *survivor*, then, is available primarily to individuals of means.

The mode of subjectivation is the second aspect of how moral subjects are constituted, and entails "the way in which people are invited or incited to recognize their obligations," whether through some kind of law, rule, or order (2003, p. 111- 112). In the Vivos solution, the mode of subjectivation operates on the site at the rhetorical level of recognizing oneself as a survivor as well as at the material and economic levels of purchasing space in a shelter, and preparing yourself with the necessary supplies to survive extreme situations. With the option to purchase shelter space aside, the discourse is quite similar to that of "prepper" discourses that center on having the plans and the means to survive society-changing scenarios (but not necessarily as part of a pre-packaged solution). In this regard, practicing the self as survivor in terms of purchasing space in a shelter makes self-forming activity, the third aspect of ethical substance, much easier. The way that we operate on our ethical substance is self-forming activity (pratique de soi/ l'ascetisme—asceticism): the ways that one might alter his or her self in order to meet the expectations of the field of morality one is operating in. Vivos works to establish the shelters as communities through promises of a careful selection process, co-ownership with other community members, and the design of the shelter itself, which features community and communal spaces as well as areas of confinement (the medical area, the detention center, the classroom) that imply a disciplinary mode of governance within the shelter. As a community, survivors would define their own ethics and determine expectations through interaction and make decisions about the extent to which they will act (and pressure others to act) in accordance with those ethics. With the space already established, community members will have an architecture within which to operate that includes a number of disciplinary sites to carry out this governance.

The fourth aspect of ethics is telos, which deals with the kind of subject that individuals are working towards being when they behave in a "moral" way (2003, p. 112). In posing the community member as "survivor" and the survivor as the ideal moral subject that sees populations through crisis, purchasing an interest in the shelter community becomes a way of buying into behaving in a moral way. In this respect, Vivos and other "turnkey" shelter solutions represent an economic answer to a moral problem that is posed as less a problem of "if" and more a problem of "what," "when," and "for how long." While these survival solutions set forth possible realities, spaces, and infrastructures for being a survivor, in practice, communities will be tasked with the process of creating a post-event ethics those members will co-construct and practice. The particular morality of surviving does not preclude the possibility of immoral or unlawful behavior, however, as evidenced by the inclusion of holding cells and vaults for storing valuables in the facilities.

In *The hermeneutics of the subject* (2005), Foucault examines the theory of the care of the self as developed in the second part of the *Alcibiades,* where he explains that Plato takes up two main questions: one concerns what the self is, and the second is concerned with the form that this care should take. Foucault examines the process by which Socrates and Alcibiades arrived at the definition of the "self as soul" through an analysis of the dialogue between them, which revolves around "uses." As Foucault explains, in this view "as the body cannot make use of itself" what uses the body "is and can only be the soul. So the subject of all these bodily, instrumental, and linguistic actions is the soul: the soul inasmuch as it uses language, tools, and the body" (p. 54).

Foucault explains the important function of the Greek verb khrēsthai, which translates into "I use" and can denote the use of objects and attitudes as well as express relationships

(as in with the gods), appropriate uses (doing something properly), and a relationship with oneself (p. 56). Foucault notes that in employing this notion of khrēsis to discover the self "it is not at all the soul-substance he discovers, but the soul-subject" (2005 p. 57). This soul as subject is distinguished from soul as substance in that in the former, one cannot care for the self except by way of a master who cares about the subject's care for the self, and the path to this self care is to acquire knowledge of the self through seeing the self through the divine. This soul-subject, Foucault explains, deals with taking care of the self "insofar as it is the "subject-of" a certain number of things: the subject of instrumental action, of relationships with other people, of behavior and attitudes in general, and the subject also of relations to one's self" (p. 57). This concept of khrēsis, or use, is particularly helpful when thinking of the subject position of being a survivor (as opposed to a survivalist). As the subject sees him/herself as the subject of an array of potential scenarios of epic proportions, "surviving" is an important practice that requires securing the space, provisions, and mindset to survive in a post-event scenario. In sustaining life, the "survivor" constitutes a soul-subject which views the self in terms of making use of the self, others, and resources in order to endure potentially catastrophic circumstances with the end goal of surviving as a moral good in and of itself. At the same time, the survivor constitutes a "smart" care of the self in which individuals are able to purchase, for a fee, a subject position that ensures morality through survival and yet does not make the same demands in renouncing their present, potentially destructive, practices that survivalism would. In this way, being a "survivor" constitutes a way of both meeting the moral obligation of survival and the productive and consumptive obligations of capitalism. A survivor might ask: "why disconnect until the last possible moment, and even when the grid is off, why go without it?"

Public-Private Preparations and Continuity of Operations

What we might call a new architecture of fear is emerging in the United States. In their report "Top Secret America: A Washington Post Investigation," journalists Bill Arkin and Dana Priest reveal a "fourth branch" of government that has emerged since 9/11 in Colorado, Alaska, Texas, Florida, Washington D.C. and the surrounding areas. With an increasing amount of persons, money, agencies and facilities committed to top-secret projects and organizations, Arkin and Priest argue that more transparency is needed in regard to these partnerships and activities. According to their video report "Growth of domestic counterterrorism," the purpose of many of the nearly 4,000 local, state, and federal agencies working on counterterrorism efforts is to "collect, store and analyze information on thousands of U.S. citizens and residents" and monitor data related to threats (2010). The report also includes a map that shows the location of government offices involved with counterterrorism efforts as well as more than 6,900 locations of 1,931 companies involved in counterterrorism and top-secret work, which are often co-located, and a detailed database of connections between various government agencies and contractors in an interactive graphic which demonstrates the hundreds of links between the government and the private sector in counterterrorism and national defense.

This emerging contractor network is changing the way that national security is thought of in important ways. As with the protection of critical infrastructure and key resources discussed in chapter three, continuity of operations, national security, and even the survival of persons is increasingly tied with financial security, investments, and private corporations. Cooperation between governments, non-governmental organizations, corporations and contractors requires us to consider efforts to ensure "survival" as largely

tied to the ability for this public-private partnership to be maintained with the backing of the military rather than the civilian population. Informationalization is a process that both emerges from and facilitates such broad-based cooperation. National security is no longer something that can be provided for by the government alone. Securing "the nation" as such also involves securing key resources and persons globally, and while governments often lack authority to carry out operations abroad, private companies enjoy more latitude. In this sense, in order to provide for continuity of operations in the event of a disaster, the government must also protect this vital public-private partnership.

That is not to say that the government has abandoned more traditional measures of continuity of operations planning: though the Greenbrier Bunker has been declassified, there is much speculation that the government continues to maintain a number of backup facilities and Deep Underground Military Bases (D.U.M.B.s). One such facility is allegedly built deep beneath the Denver International Airport, and another is said to exist at Cheyenne Mountain (the bunker housing the fictional stargate device in the *Stargate* franchise). Conspiracy theorists online have speculated (and attempt to offer evidence) that these D.U.M.B.s are networked with advanced underground transportation systems and are stocked with food and supplies as well as equipped with the capabilities of growing food underground (think of the bio-domes in *Silent Running* (1972), but carved into rock). The message is consistent: these facilities are for government and military personnel as well as "the elite" (including high-level military consultants and contractors) while the American People will be in a FEMA camp (if they are lucky). Many of these claims are supported by little evidence – there are few pictures, and most of the information is gathered from anonymous sources. Then again,

until the Greenbrier facility was de-classified, most information came from anonymous sources, hearsay, and speculation.

In a 2010 episode of TruTV's *Conspiracy Theory with Jesse Ventura*, host and former actor, wrestler, and Governor of Minnesota Jessie Ventura chases down a series of clues about a deep underground military base located under the Denver Airport. The secret base is reported to be accessible via the military base at Cheyenne Mountain Air Force Base outside of Colorado Springs, Colorado. According to the Denver International Airport website, the airport opened on February 28, 1995 and is the only major airport built in the U.S. in the last 25 years. The facility's website explains that while "Some people think there's a conspiracy making our airport the center of a New World Order. Rest assured the story is definitely a myth" (Denver International Airport, 2011). On a visit to the grounds of Denver International Airport, video evidence suggests that digging and building is still going on at the site. Ventura says, "Government Bunkers? They're no secret. The only thing we don't know is how many, and where" (2009).

No known shelter network exists to provide for the more than 300 million people living in the United States today. The shelter solutions discussed in this chapter, while appropriate for the privileged and necessarily financially solvent smart subject, do not provide for the majority of the people that the United States government is charged to protect from threats both domestic and foreign. At more than $25,000 per person, space in a Vivos shelter is out of reach for the majority of citizens. Without the benefit of thousands of dollars of disposable income, preparation for disaster looks less like a cruise ship buried underground and more like a few gallons of potable water and a first aid kit.

The U.S. Federal Emergency Management Agency suggests rather that citizens prepare with the assistance of a 204 page document titled *Are You Ready?* last updated in 2004. The document is available for download on their website and outlines responses for scenarios under three main categories: Natural Hazards, Technological Hazards, and Terrorism. Included in the appendixes is the Department of Homeland Security "Family Communications Plan" which provides space to record contact information; name, date of birth, social security number and medical information for family members; and addresses for places of work and schools. The final section of the form provides space to record "important information" including the name, phone number and policy number for the following: Doctor, Other, Pharmacist, Medical Insurance, Homeowners/Rental Insurance, and Veterinarian/Kennel (for pets). A separate page includes wallet size forms to record important information to be kept with the individual at all times. Recording such information as part of a plan assumes that communication and transportation networks are still viable, and does not provide for scenarios such as infrastructure failure brought about by solar flares, cyberattack of critical infrastructures, or cyber or infrastructure war. Citizens can only hope that the sectoral plans developed as part of a public-private partnership to protect critical infrastructures are robust enough to be effective.

Conclusion: The Informationalized Infrastructural Ideal

In this dissertation, I have analyzed utopian (smart) and dystopian (critical) discourses of informationalization across a variety of scales and platforms in order to explore the ways in which a range of infrastructures have become increasingly entwined with communication and information. Seeing informationalization as a driving growth in markets based on the effective movement of information, energy, people and objects, I have examined cases with intersections in energy, transportation, government and (in a sense) housing in order to demonstrate the wide reaching implications of the informationalization of infrastructure for life in the United States. What moves across infrastructure seems to matter less than if that transit/transmission is profitable, secure, and rational, be it millions of automobiles, hundreds of exabytes of digital data that move across the internet globally every year, or the trillions of dollars that move between banks each day. Like fish in water, information, objects, people, communication and money need to *flow.* Informationalization helps corporations, governments, and even consumers to better manage production, distribution and consumption of such flows. Processes of informationalization work on the one hand to create new market opportunities in transmission and on the other hand to work to secure such markets. Having mapped "smart" and "critical" discourses of informationalization, I next discuss the new infrastructural ideal and an associated politics of security that is coextensive with both utopian and dystopian discourses of informationalization.

The Modern Infrastructural Ideal and *Splintering Urbanism*

The modern infrastructural ideal, which Graham and Marvin (2001) explain saw infrastructures at the scale of the city as "mechanisms to control time through instigating waves of societal progress," was supported by four larger trends: progress and modernization, modern urban planning, home-based consumption and government provision of public infrastructure (pp. 42-43). They explain that as infrastructure began to be seen as a means for achieving progress, it came to be seen as a central component in modernization of the city, playing into larger notions of the technological sublime. They further explain that following the emergence of centralized infrastructure, urban planning movements began to take hold that sought to rationalize the city through the effective management of its space, achieved in part through infrastructure. The third pillar of this ideal lies in the ways that ideas of progress and planning "came together to support new types of mass production and consumption between 1920 and 1960, mediated by standard networks in the city" (p. 66). This move to the "mass" can be seen as one accompanied by not only transportation and utilities infrastructures, but also an increase in mass communication options including radio and television and larger trends such as mobile privatization (Williams, 1974/2003). The last pillar of the modern ideal is government focus on universal access to and regulation of infrastructure, often leading to a vision of some infrastructures as natural monopolies.

Graham and Marvin explain that this ideal was problematized by a series of interrelated factors beginning in the late 1960s, including a crisis in urban infrastructure as spending on infrastructure failed to keep pace with development and repair needs; moves toward globalization and privatization of infrastructure; a move from plans to projects in urban planning; growth of geographical regions; and various social movements including the

environmental movement (pp. 91-136). They argue that processes of splintering urbanism driven largely by the unbundling of infrastructure through changing economic conditions, the integration of control systems in infrastructure and improvements in quality of service and transmission have eroded the modern infrastructural ideal, opening up new possibilities for the management of infrastructure. They argue that these processes and their implications for life in urban areas must continue to create frameworks for understanding the "splintered metropolis" (p. 406).

The Informationalized Infrastructural Ideal

Graham and Marvin's splintering urbanism describes a process of deterritorialization that set the stage for a reterritorialization of infrastructure. I argue that the informationalized infrastructural ideal represents an intensification of such processes of splintering urbanism that has been accompanied by advances in communication, transportation and information technologies, a broader cultural move that sees processes of informationalization as "smart" more broadly, and a desire to open up new markets in transmission and distribution of products and services.

This dissertation has explored processes of informationalization across three main case examples: Better Place's electric automobility platform, Stuxnet as cyber ordnance and the increased focus on critical infrastructure protection and cybersecurity, and finally at community survival solutions. Throughout these cases, informationalization is posed as a means to a smarter car, smarter war and defense, and even a smarter subject that leverages connectivity even after breaking connection with the larger energy, communication, economic and social grid. These cases point to the emergence of a new infrastructural ideal

which is converged rather than splintered and centralized not at the point of city planners or governments, but rather around the individual subject who can leverage technologies of screening from cell phones and smart meters to dashboard displays to monitor their own production and consumption (Packer & Oswald, 2010). These technologies serve as access points for managing oneself as a citizen of the "Smarter Planet" – in a sense, even subjects have been swept up in the move to "1. Instrument the world's systems; 2. Interconnect them; and 3. Make them intelligent" (IBM, 2011b). Despite the many advantages to informationalization discussed by invested corporations, governments, technophiles and the media, there are downsides and challenges to such connectivity.

A main challenge in the informationalized infrastructural ideal is in negotiating the tension between connection and security by leveraging logics of screening and control—to connect infrastructure, but to be able to discern safe and unsafe use and desirable and undesirable access and use—using the "sight" provided by informationalized networks to manage and defend them. As informationalization opens up new opportunities for connection, security becomes a critical element in the design, development, and protection of infrastructures. Next I present the "fire sale" as one last example of the imagined risks of informationalized infrastructure, exploring the roots of what became the central plot for *Live Free or Die Hard* (2007) in government crisis-planning exercises. In summary, the central plot of the film is to locate and stop terrorists that have exploited informationalized infrastructure (transportation, communication, and utilities) so as to throw the United States into crisis. While this movie is fictional, it is based on the potential for informationalized infrastructure to succumb to cyberattack that could come at any time, from anywhere, without warning (as was the case with Stuxnet, discussed in chapter three).

Fire Sale: Everything Must Go!

A key site for thinking about infrastructure networking and failure is through the idea of the *fire sale* that served as the central plot point in the 2007 film *Live Free or Die Hard*. The origins of this concept are in an actual disaster scenario, "The Day After," run by the FBI, DOD and NSA. While the phrase "The Day After" may conjure the specter of the atomic bomb, a fallout cloud hanging over burned bodies and buildings in ruins or the 1983 made-for-television movie of the same name, in this case it refers to a long-standing disaster response scenario played out in Washington D.C. that for years had at its center the threat of nuclear war. When the scenario was run in the 1990s, officials were no longer focusing on the atomic bomb; instead, as John Carlin's 1997 article discusses, they were preparing for information war, which not only demands new strategies and tactics, but calls the very nature of war into question:

> [T]he landscape is vast, hard to visualize, and infinitely flexible. I-war can be the kind of neat, conceptually contained electronic Pearl Harbor scenario that Washington strategists like - collapsing power grids, a stock market software bomb (Tom Clancy's been there already), an electromagnetic pulse that takes the phone system out. Or it could be something completely different: An unreachable, maybe even unknown, foe. Grinding you down. Messing with your collective mind. Driving you slowly, gently nuts. (para. 19)

Carlin explained that the Pentagon was largely unready for such attacks, but explains that as of 1997, they were taking a number of steps to prepare for information warfare. First, the Pentagon pushed for tightened security of military networks, more extensive training for information war, and the development of a program to monitor attacks on civilian infrastructure. Second, they shifted much of the responsibility to local law enforcement and the intelligence community (how can information war be considered a military concern?). Carlin writes that the task of securing the national infrastructure is more complicated than it

seems, as global, national, and military networks are nearly indistinguishable and the physical infrastructure is in corporate rather than government hands.

The rights to Carlin's article "Farewell to Arms" were purchased to be developed into a movie titled *WW3.com* set to be released in summer 1999. The film was scrapped, but the plot later surfaced in *Live Free or Die Hard* (2007), the fourth installment of the Die Hard franchise. As this article and much of the RAND and DOD literature demonstrates, the idea of a simultaneous attack on multiple infrastructures via information networks pre-dates 9/11, though research around the topic has certainly intensified since. Arquilla & Ronfeld's *NETWAR*, which classifies, explains, and elaborates network forms and identifies specific policy challenges, was published in 1996: the same year as *Shock and Awe: Achieving Rapid Dominance.* In the realm of specific applications, Chun points out in *Control and Freedom* (2006) that the U.S. was bombing Iraq in the late 90s for developing a fiber optic infrastructure –securing the superiority of our network over others by denying the networking of another state. Grahams' (2009) recent work highlights the practice of urban infrastructure warfare in U.S. military operations abroad as early as the Gulf War, in which the targeting of "dual-use infrastructures"— those considered both civilian and military—were carried out as part of larger strategies to destabilize territory. An emerging capability for cyber-based delivery of such effects complicates the international legality of such strategies, as it is makes it increasingly difficult to identify the origin, direction, or duration of an attack. The only defense is constant vigilance and designing systems to be impervious, flexible, or quickly restored in case of attack.

Live Free or Die Hard

The *Die Hard* series has always been about security and infrastructure. New York City cop John McLane, protecting family and homeland from terrorism, fights those who attack infrastructure by exploiting areas of maintenance and repair (elevator and ventilation shafts, sewer system) in order to secure an office building (*Die Hard*, 1988), an airport (*Die Harder*, 1990), and a city (*Die Hard with a Vengeance*, 1995). In some particularly exceptional scenes involving uses of infrastructure for unintended purposes in the fourth installment in the series, *Live Free or Die Hard* (2007), McLane destroys a helicopter by driving a car into a toll booth (sending it skyward); plows through the corridors of a power station in an SUV; and avoids being destroyed by an F-35 while driving a tractor trailer as the road beneath him crumbles by jumping out of the cab, landing on a jet, and sliding down a broken segment of road. The central plot of the film makes an interesting variation on the theme in a number of ways, as McLane fights a mobile fleet of cyberterrorists working to systematically take down critical utility, communication, and transportation infrastructures in order to steal billions of dollars.

In phase one of the attack, cyberterrorists cause mayhem as all Washington, D.C. traffic signals turn green (transforming intersections into spaces of collision rather than interchange), Amtrak and the FAA report technical malfunctions, and federal buildings including the FBI building and Capitol Building are emptied through the false trigger of anthrax alarms. In the second stage, the terrorists crash the financial system and deliver a "video package": a mash up of presidential speeches delivering a message designed to instill terror while at the same time perverting and de-legitimizing the office of the president,

followed by a convincing simulation of the destruction of the Capitol Building. Soon after, McLane's hacker sidekick Matt Farrell explains that what is taking place is a "fire sale," a:

> …three-step systematic attack on the entire national infrastructure. Okay, step one: take out all the transportation. Step two: the financial base and telecoms. Step three: You get rid of all the utilities. Gas, water, electric, nuclear. Pretty much anything that's run by computers, which today is almost everything. So that's why they call it a fire sale: because everything must go.

We later learn that purpose of this attack was to set off a chain of events that would cause the national financial data to begin to be backed up by a National Security Agency failsafe program at the Social Security data centers in Woodlawn, Maryland. Thomas Gabriel, disgruntled former Chief Programmer for Infrastructure Security at the Department of Defense is the architect of both the "fire sale" and the backup system. It is explained that Gabriel called for a security overhaul, and when DOD officials did not take him seriously, he took down NORAD (the North American Aerospace Defense Command) systems with a laptop, was dismissed, and went off the grid. Toward the end of the film, Gabriel explains that he is trying to help—"Better me than some outsider. Some religious nut job bent on Armageddon. Nobody wants to see that happen. Everything I've broken can be fixed if the country is willing to pay for it."

Given the difference between "Farewell to Arms" (1997) and *Live Free or Die Hard* (2007), it is understandable why Carlin made a point to correct reviews that claimed the movie was based off of his article. While this is understandable, a movie about the "Day After" scenarios involving the FBI, DOD, DARPA and RAND, is not the kind of story that sells movie tickets, at least not during summer blockbuster season. That said, there is a striking similarity between the way that Carlin almost playfully describes the forms that

information war can take—as either systematic and calculated or messy and chaotic—which are demonstrated clearly in Gabriel's superior attitude and vengeful motivations.

Fire Sale

While the concept of a "fire sale" as a three pronged infrastructure attack may have become much more widely disseminated via *Live Free or Die Hard*, the concepts are clearly being developed in Carlin's article and (more significantly) in the Department of Homeland Security, DOD, FBI, NSA, and a host of other groups, corporations, organizations, and inter-departmental agencies. One should not think of military doctrines such as Rapid Dominance, Critical Infrastructure, Shock and Awe, Infrastructure Warfare and Cyberterrorism as post-9/11 phenomena; it is important to recognize their origins in a longer trajectory of military research and programs. This research intends to locate and explore the origins of these logics in order to understand them as part of a continued development in U.S. military thinking about infrastructure, warfare, and security.

I was unable to locate any academic or popular press articles using the term "fire sale" to describe infrastructure attack scenarios before 2007, which leads me to believe that the phrase was conceived in the script-writing or production phase as a way to describe coordinated infrastructure attack. The term generally deals with financial closeouts and liquidations: where "everything must go," which demonstrates a common thread between the terms – one stands for financial ruin, the other, the ruin of infrastructure. In both cases, the term points to a breakdown in security: in the first sense economic and the second national. The use of the term to describe the simultaneous attack of multiple infrastructure networks remotely articulates a strategy of infrastructural warfare and explains an emerging

configuration of homeland security that re-visions infrastructure as "critical" in a digitally networked and converged context. As *the simultaneous immobilization of multiple critical infrastructures*, in the "fire sale" infrastructure can be seen simultaneously as smart and critical. The link between the two kinds of securitization is also clear in government policy that also looks to protect "key assets" through public-private "partnerships" and investment in security/security in investments.

The "fire sale" highlights the central role of infrastructure in national, urban, and social space, and is one way of considering infrastructure not as boring, unimportant, or dead, but enabling, critical, and active. Second, the depictions of the state of infrastructure securitization through the fire sale demonstrate an underprepared and nearly helpless general populace, save those individuals who can either contribute to security by making the self safe (the smart subject) or making the nation safe (COOP). Third, disconnection is oddly not presented as a response; though operating outside of networked infrastructure seems the easiest way to minimize effects of collapse. Last, while both depict a version of security, the focus is on both infrastructure and financial data, significant in that there appears to be a shift in focus from the population to the network, perhaps best understood in the context of Foucault's governmentality and Deleuze's conception of "societies of control."

Governmental Logic

Michel Foucault wrote *Discipline and Punish* as a response to and an argument for prison reform, tying his work to a political struggle. This work represents the foundation of Foucault's analysis of forms of power and power relations, as he explores the emergence of disciplinary power in sovereign power relations. He explains that while sovereign power is

the kind of power enacted by a sovereign and happens through transparent and spectacular displays of violence on subjects that work to restore power, disciplinary power is effected less through the taking and granting of life than the shaping and structuring of behavior through institutions. Foucault looks to prisons, schools, and barracks as sites of disciplinary power that shape life: subjects must be at designated places at certain times for prescribed purposes. The idea of Bentham's Panopticon here is an important one – Foucault explains in an interview in *Power/Knowledge* (1980) that his focus on the Panopticon centered on the fact that it was a way of thinking about structuring a space that came to be pervasive in hospitals, prisons, and other institutions where people were meant to both watch one another as well as be watched without knowing who was watching (or if anyone was watching at all). In this sense, power is *immanent*.

Foucault later considers power in the move to "governmentality," which he develops in a series of lectures at the Collége de France, published later as *Security, Territory, Population* (2007). He explains that with governmentality, the move to a focus on managing at the level of population operates all over and at all levels and that the "state" actually operates and came to be through logics of governmentality. Governmentality has a focus on security rather than disciplinarity, and does not "replace" disciplinary and sovereign powers but rather is coextensive with them. Tied to this notion of governmentality is the concept of "pastoral power;" the church recognizes their ability to manage the population, and the state uses that technique (Foucault, 1988). Exploring the manner by which individuals practiced the self in ancient Greece and during early Christianity, he examines practices such as Stoic techniques of mental preparation and early Christian practices of penitence and self-proclamation to understand the origins of the form of governmental power.

Bratich, Packer and McCarthy (2003) explain that governmentality "takes place at innumerable sites, through an array of techniques and programs that are usually defined as cultural" as opposed to techniques and apparatuses of the State, and that the role of the state in governmentality is "one of coordination, one that gathers together disparate technologies of governing inhabiting many sites" (p. 4-5). They argue that governmentality as an analytic can bring to the surface certain cultural formations as important sites for cultural studies. Following this, we must be attentive to new forms of power operating in networks, particularly where previous understandings of the operation of power cease to explain the technosocial milieu. One other such approach that has been brought to understanding new forms of power is Deleuze's conception of the "control society."

Societies of Control

Work discussing governmental conceptualizations runs parallel to Deleuze's conceptualization of control societies: though addressing similar topics and concerns, work in these veins rarely intersects. Though *Foucault* (1986) was written two years after Foucault's death, Deleuze makes no mention of Foucault's late work on governmentality. Writing about the relation between the subject and power, Deleuze reinterprets Foucault's care of the self as a process of folding, and writes that "there never 'remains' anything of the subject, since he is to be created on each occasion, like a focal point of resistance, on the basis of the folds which subjectivize knowledge and bend each power" (p. 105). Perhaps this focus on technologies of the self as folding is what takes Deleuze away from Foucault's discussion of governmentality, which Foucault situates as the "encounter between the technologies of domination of others and those of the self" (2003, p. 147).

In “Postscript on control societies” (1997), Deleuze discusses a shift in thinking from discipline to control rather than discipline to governmentality. Many scholars across a variety of disciplines have used Deleuze’s conceptualization of “societies of control” as a jumping off point to describe the ways that the present environment is increasingly controlled (for better or worse). Deleuze explains the difference between discipline and control throughout, arguing that control society modulates rather than confines, uses codes and passwords rather than signatures and numbers, and rethinks the individual in terms of a *dividual*, and the mass in terms of database (p. 180). Making a connection between control and cybernetic machines, he stresses the importance of understanding of “the basic sociotechnological principles of control mechanisms as their age dawns,” and suggests that these principles be used to describe “what is already taking the place of the disciplinary sites of confinement that everyone says are breaking down" (p. 182). In this call to describe mechanisms, we can see another difference: Deleuze focuses on process, movement, and mechanisms where Foucault is interested in power, practices, and institutions.

Which analytic is more useful—governmentality, which looks to the conduct of the self in terms of institutions that work to organize practice? Or control, which instead looks to societies’ machines in order to understand the ways power operates? This project has worked to examine informationalization in terms of both practices and machines, as its processes clearly affect both. I have explored governmental aspects of this process where the practice of the self has met with practices of power at the level of population in terms of critical infrastructure protection and neoliberal survival solutions. Seeing critical infrastructure as a way of thinking about protecting infrastructures at the level of population, plans and programs to secure infrastructure have stressed public-private cooperation and a shift from

ensuring the safety of infrastructure to one of increased security. An examination of survival solutions served as a case example for a much longer trend for the government, which provides for itself through continuity of operations planning, to direct citizens to care for the self in a particular way through the provision of information, plans, and blueprints for shelters rather than the shelters themselves. In these examples, a governmental framework has helped to describe constructions such as the smart subject and highlight the central role of the private sector in national, domestic, and critical infrastructure security.

Following Deleuze's suggestion in "Postscript on societies of control" I have also worked to describe the mechanisms and capabilities of informationalization. In the case of automobility, I examined the role of informationalization in making possible a market-viable electric automobility solution. Looking historically at electrically powered mobility, I examined the role of informationalization in the creation of a nexus system that drives like a series system and discussed both the promises and challenges of such a system that would come from larger-scale implementation. Additionally, the same chapter considered the potentials for continued informationalization of the automobile as a space increasingly fitted with control mechanisms. The examination of Stuxnet in chapter three looked specifically at cyber ordnance as a new mechanism of war, and explored the need for system creators and owners to become involved in national security efforts as critical infrastructures become increasingly informationalized. Finally, I examined community shelter spaces as mechanisms for survival in the informationalized infrastructural ideal.

Neither Foucault's governmentality nor Deleuze's societies of control are effective in totally explaining informationalization that involves practices and machines, net-work and networks, biopower and electrical power. As informationalization continues to make

infrastructures, systems, and grids "smart," it is crucial to observe existing arrangements in order to begin to understand the ways that power works in these assemblages: while theories of power can serve as a guide, we must turn our attention instead to what is new and different about the ways that power operates in infrastructures and systems in specific contexts. My goal has been to locate informationalization in a variety of contexts to better understand the way it affects communication, mobility, security, war and survival as a starting point for continuing to examine the effects of such a process.

A Smarter Solution

In working to reduce ambiguity in research about and around informationalized infrastructure, chapter one of this dissertation served as a starting point in defining central terms such as infrastructure, system, network, grid, informationalization and smart. With these terms clarified, conversations about informationalization can progress in a more coherent fashion across disciplines. My focus in defining these terms is both disciplinarily broad and phenomena specific. While the field of communication is perhaps best suited to lead efforts in understanding informationalization, cooperation with fields such as geography, mobilities studies, information science, engineering and sociology is necessary to more fully understand the ways that information is fundamentally changing the ways that we interact with space, movement, information, systems and society more largely. To make steps toward such interdisciplinary collaboration, the definitions provided here are specific to changes brought about by the addition of information to processes rather than specific disciplinary concerns.

The rhetoric of the smart sublime suggests that the world can be made better through a process of informationalization. While "smart" in this sense refers to moves to informationalize for its own sake, informationalization can also be leveraged to make systems smart in another sense: better for consumers, citizens, and the environment. Following an assemblage view of systems, I argue that we must locate possibilities within the informationalized infrastructural ideal to map coextensive articulations of infrastructure that do not necessarily require the undoing of smart infrastructure and security, but rather meet the objectives of a smarter planet in more than one narrow sense of the term. Chapter two argues that we continue to question (or as Carey suggests, demystify) the smart sublime by looking past the potential for technology to save us and instead at what such technologies make possible and what "smart" has come to represent in discourses of the smart sublime.

My analysis of Stuxnet and pre- and post-9/11 discourses of critical infrastructure protection and cybersecurity in chapter three suggested that "smart security" in the form of public-private partnership is in fact not a post-9/11 phenomena, but rather one that emerged in a context of increased reliance on the communication networks of the private sector and informationalization across a plethora of systems and processes. As an increasing number of infrastructure sectors are informationalized and the threat of cyberattack continues to grow, public and private sector cooperation will be more and more important. With Stuxnet proving the potential for attack on physical infrastructure to be delivered via communication and information networks, this partnership will become increasingly critical in itself. It is important to examine the ways in which this PPPs will evolve in a post-Stuxnet environment, and the lens of smart security will prove useful in thinking about national and economic security in an informationalized infrastructural ideal.

Through an analysis of the infrastructures of survival in chapter four, I discussed disconnection from "the grid" and examined spaces of survival more specifically. Through this analysis, I discussed in detail the emergence of a "smart subject" who, rather than learning to live without the grid in anticipation of disaster (natural, unnatural or otherwise), instead supplies him/herself with a grid-away-from-the-grid alternative. Through an examination of Foucault's *technologies of the self* and later work on the hermeneutics of the subject, I demonstrated how commercial solutions are presented by private companies to present survival as a moral good that could be smartly achieved through co-ownership in a community shelter without all the "inconveniences" of a variety of brands of survivalism. In this case, as in the others, smart is a value-added proposition that seemingly nudges us toward a society more fitting in to informationalization rather than informationalization more fitting itself to society.

As the work of scholars including Raymond Williams (1974/2003), James Carey (1989), Langdon Winner (1986) and Henri Lefebvre (1991) suggests, early choices made by engineers, planners, government officials and invested corporations, whether intentional or not, hold strong influence over the ultimate shape and use of systems. When faced with a challenging project, my M.A. adviser once asked me to imagine any project in terms of a painting where each brush stroke influences the next: eventually the canvas is full of paint, and even the painted-over sections have had an impact on the painting as a whole.

Following this, we might imagine informationalization as a process of scanning that painting and creating a digital file that can be cropped, sharpened, and otherwise modified without altering the original. Seeing informationalization of infrastructure as one way that the possibilities of such flexible modification can radically expand the possibilities of systems, it

is critical that scholars, activists, and citizens continue to examine the digital modifications being made by the new editors of systems. It means that we must question editorial decisions of those who modify systems as "smart" and to ask whether such modifications truly result in better outcomes for communities, citizens and users or merely more productive investments (Better Place), more secure financial and national interests (critical infrastructure), or one more way for governments to shift responsibility to citizens (Vivos Group). We must not only question these cases, but also imagine ways that the same processes of informationalization can be leveraged in ways to make services more accessible, affordable, and safe: to make them truly *smart*.

Bibliography

20th Century Castles LLC (2011). Available at: http://www.missilebases.com/adironback

Agamben, G. (2009). *What is an apparatus?* Palo Alto, CA: Stanford University

Alden, H. W. (1923). Reviews of report of committee on bus operation. *Electric Railway Journal*, *62*(15) 602-603. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/602/mode/2up

Anderson, C. (2010). The web is dead. *Wired*, *18*(9) 118-127; 164.

Arkin, W. M. & Priest, D. (2010). Top secret America: A Washington Post investigation [website]. Retrieved from http://projects.washingtonpost.com/top-secret-america/

Arquilla, J. & Ronfeld, D. (1996). The advent of Netwar: A RAND monograph report. Retrieved from http://www.rand.org/pubs/monograph_reports/MR789/

Bajc, V. (2010). Security meta-framing: A cultural logic of an ordering practice. In V. Bajc and W. de Lint (Eds.) *Security and Everyday Life* (pp. 1 -30). New York and Oxon, U.K.: Routledge.

BBC News (2010, September 26). Stuxnet worm hits Iran nuclear plant staff computers. BBC News Middle East. Retrieved from http://www.bbc.co.uk/news/world-middle-east-11414483

Banks, D. O. (2001). Information War Crimes: Mitnick meets Milosevic. Retrieved from the Storming Media database. (A892604).

Beaumont, C. (2010, September 23). Stuxnet virus: worm 'could be aimed at high-profile Iranian targets'. *The Telegraph.* Retrieved from http://www.telegraph.co.uk/technology/news/8021102/Stuxnet-virus-worm-could-be-aimed-at-high-profile-Iranian-targets.html

Bentley, J. & Derby, R. (2002). Ethanol & fuel cells: Converging paths of opportunity [white paper]. Retrieved from http://www.ethanolrfa.org/page/-/rfa-association-site/studies/fuelcells.pdf?nocdn=1

Best, K. (2003). The hacker's challenge: Active access to information, visceral democracy and discursive practice. *Social Semiotics, 13*(3), 263-282.

Better Place (2011). Betterplace.com [website]. Retrieved from http://www.betterplace.com

Better Place (2011, March 23). Better Place unveils network deployment roadmap for Israel, offering electric car drivers complete nationwide coverage by end of year [press release]. Retrieved from http://www.betterplace.com/the-company-pressroom

Bhattacharjee, Y. (2011). Why does a remote town in Romania have so many cybercriminals?. *Wired, 19*(02) 82-87, 124.

Biello, D. (2009, May 8). R.I.P. hydrogen economy? Obama cuts hydrogen car funding. *Scientific American News Blog.* Retrieved from http://www.scientificamerican.com/blog/post.cfm?id=rip-hydrogen-economy-obama-cuts-hyd-2009-05-08

Blondheim, M. (1994). *News over the wires: The telegraph and the flow of public information in America, 1844-1897*. Cambridge, MA: Harvard University Press.

BP (2004, May 19). First to Provide Hydrogen at Existing Filling Station [Press Release]. Retrieved May 21, 2010 from http://www.bp.com/genericarticle.do?categoryId=2012968&contentId=2018380

Bradley, D. A. (2004). Dimensions Vary: Technology, Space and Power in the 20th Century Office. *Topia 11*, 67-82.

Bratich, J. (2011). User-generated discontent. Cultural Studies 25(4-5) 621-640.

Bratich, J., Packer, J. & McCarthy, C. (2003). *Foucault, cultural studies, and governmentality*. Albany, NY: SUNY Press.

Brown, D. (2010, April 28). Lithium development in Bolivia heats up. Lithium Investing News (website). Retrieved from: http://lithiuminvestingnews.com/1216/lithium-development-in-bolivia-heats-up/

Broad, W. J., Markoff, J. & Sanger, D. E. (2011, January 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *The New York Times.* Retrieved from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Buick (2011). Buick LaCrosse OnStar Mobile App Lets Access your Vehicle From Your Smart Phone [video]. Retrieved from http://www.youtube.com/user/buickdfw

Busses Replace Cars (1930, June). Busses Replace Cars In Local Service at Patterson. *Electric Railway Journal, 74*(6) 315-317. Retrieved from http://www.archive.org/stream/electricrailwayj742mcgrrich#page/314/mode/2up

Cameron Gulbransen Kids Transportation Safety Act of 2007. 49 U.S. C. § 30111.

Catlaw, T. J. (2008). Governance and networks at the limits of representation. *The American Review of Public Administration, 39*(5), 478-498.

Carey, J. (2005). Historical pragmatism and the internet. *New Media & Society 7*(4), 443-455.

Carey, J. (1989). *Communication as culture: Essays on media and society.* Boston: Unwin Hyman.

Carey, J. and Quirk, J. (1970/1989) The mythos of the electronic revolution. In J. Carey (Ed.) *Communication as culture: Essays on media and society.* Boston: Unwin Hyman.

Carey, T. (2010). The cleantech revolution. *View, 12.* 49-61. Retrieved from http://www.pwc.com/en_US/us/view/assets/pwc-view-issue12.pdf

Carlin, J. (1997). A Farewell to Arms. *Wired. 5*(05). Retrieved from http://www.wired.com/wired/archive/5.05/netizen.html.

Castells, M. (2000). *The rise of the networked society* (2nd Ed.). Malden, MA: Blackwell.

Chambers, N. (2008, July 24). How to Build an Electric Car Charging Infrastructure: Smart Grids, Fast Charging and Universal Access. *Gas 2.0.* Retrieved from Intelligent charging infrastructure: http://gas2.org/2008/07/24/how-to-build-an-electric-car-charging-infrastructure-smart-grids-fast-charging-and-universal-access/

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24*(2), 229-251.

Chevrolet (2011). 2011 Volt: It's more car than electric [website]. Retrieved from http://www.chevrolet.com/volt/

Chow-White, P. A. (2008). The informationalization of race: Communication technologies and the human genome in the digital age. *International Journal of Communication, 2* 1168-1194. Retrieved from http://www.ijoc.org/ojs/index.php/ijoc/article/viewFile/221/243

Chun, W. K. H. (2006). *Control and freedom: Power and paranoia in the age of fiber optics*. Cambridge, MA.: MIT Press.

Clayton, M. (September 21, 2010). Stuxnet malware is 'weapon' out to destroy... Iran's Bushehr nuclear plant? *The Christian Science Monitor*. Retrieved from http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

Colomar-Garcia, M. & Zhao, X. (April 23, 2011). Tapping Latin America's lithium. *Latin Business Chronicle*. Retrieved from http://www.latinbusinesschronicle.com/app/article.aspx?id=4855

Computer Fraud and Abuse Act (CFAA) of 1986. 18 U.S.C. § 1030.

Consumer Assistance to Recycle and Save Act of 2009. 49 U.S.C. § 32901 (2009).

Contos, B. T. (2007). *Enemy at the water cooler: True stories of insider threats and enterprise security management countermeasures*. Rockland, MA: Syngress

Cowen, D. (2009). Containing insecurity: US port cities and the 'War on Terror'. In S. Graham (Ed.) *Disrupted Cities: When infrastructure fails* (pp. 69-84). New York and London: Routledge.

Cowen, D. (2011, March). Rough trade: Cities and citizenship in the supply chain. Keynote speech presented at Mobilities in Motion: New Approaches to Emergent and Future Mobilities, Drexel University, Philadelphia, PA.

Deeter, J. (Producer), & Paine, C. (Director). (2006). *Who killed the electric car?* [Film]. United States: Sony Pictures Classics.

DeLanda, M. (2006). *A new philosophy of society: Assemblage theory and social complexity*. London and New York: Continuum.

Deleuze, G. (1986). *Foucault*. Minneapolis, MN: University of Minnesota Press.

Deleuze, G. (1997). Postscript on control societies. In G. Deleuze *Negotiations*: *1972-1990* (pp. 177-182). New York: Columbia University Press.

Deleuze, G. & Guattari, F. (1972/1983). *Anti-Oedipus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.

Deleuze, G. & Guattari, F. (1980/1987). *A thousand plateaus: Capitalism and schizophrenia*. Minneapolis: University of Minnesota Press.

Denver International Airport (2011). Do you know DIA? Retrieved from http://flydenver.com/doyouknowdia

Digital Millennium Copyright Act (DMCA) of 1998. 17 U.S.C. §§ 1201-1205.

Douglas, S. (1987). *Inventing American broadcasting: 1899-1922*. Baltimore: Johns Hopkins University Press.

Dourish, P. (2007). Seeing like an interface. OzCHI 2007, 28-30 November 2007, Adelaide, Australia.

Eads, S., Fottrell, M., Rifkin, A., & Wisher, W. (Producers), & Wiseman, L. (Director). (2007). *Live Free or Die Hard* [Motion picture]. United States: Twentieth Century Fox Film Corporation.

Electric Auto Association (n.d.). *EV History*. Last accessed February 14, 2011. Retrieved from http://www.electricauto.org/?page=EVHistory

Electronic Communications Privacy Act (ECPA) of 1986. 18 U.S.C. §§2510-22, 2701-11, 3121-26.

Ellison, N. B., Steinfield, C. and Lampe, C. (2007). The benefits of Facebook "Friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*, 1143–1168.

Emerson, R. W. (1923, October 20). Automobile accidents from transportation standpoint. *Electric Railway Journal 62*(16) 682-684. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/682/mode/2up

Executive Order No. 13,228 (2001). Retrieved from http://www.archives.gov/federal-register/executive-orders/2001-wbush.html

Executive Order No. 13,231 (2001). Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr18oc01-139.pdf

Eyrich, N., Padman, M. L., Sweetser, K. D. (2008). PR practitioners' use of social media tools and communication technology. *Public Relations Review, 34*(4) 412-414.

Falkenrath, R. A. (2011, January 26). From bullets to megabytes. *New York Times*. Retrieved from http://www.nytimes.com/2011/01/27/opinion/27falkenrath.html?hp

Federal Highway Administration (2011). Highway Statistics 2009 [Tables DL-1C, VM-203, HM-20]. Retrieved from http://www.fhwa.dot.gov/policyinformation/statistics/2009/

Foucault, M. (2007). *Security territory population: Lectures at the Collège de France 1977-1978*. New York: Pallgrave MacMillan.

Foucault, M. (2005). *The Hermeneutics of the subject: Lectures at the College de France 1981-1982*. Burchell, G., trans. London: Palgrave Macmillan.

Foucault, M. (2003). *Society must be defended: Lectures at the Collège de France, 1975-1976*. New York: Pallgrave MacMillan.

Foucault, M. (2003). Technologies of the self. In P. Rabinow and N. Rose *The Essential Foucault* (pp. 145-169). New York: The New Press.

Foucault, M. (1988). *The care of the self: The history of sexuality*. New York: Vintage Books.

Foucault, M. (1980). *Power/knowledge: Selected interviews and other writings, 1972-1977*. New York: Pantheon.

Foucault, M., Rabinow, P. & Dreyfus, H. (2003). On the genealogy of ethics: An overview of work in progress. In P. Rabinow and N. Rose *The Essential Foucault* (pp. 102-125). New York: The New Press.

Galloway, A. R. & Thacker, E. (2007). *The exploit: A theory of networks.* Minneapolis, MN: University of Minnesota Press.

Gonzalez, A. (2005, April 5). Oversight of the USA PATRIOT Act [testimony]. Retrieved from the Federation of American Scientists website: http://www.fas.org/irp/congress/2005_hr/040505gonzales.html

Graham, S. (2005). Switching cities off: Urban infrastructure and US air power. *City, 9*(2), 169-193.

Graham, S. (Ed.). (2009). *Disrupted cities: When infrastructure fails.* New York: Routledge.

Graham, S. (2010). *Cities under siege: The new military urbanism*. London & New York: Verso.

Graham, S., & Marvin, S. (2001). *Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition.* New York: Routledge.

Graham, S. & Thrift, N. (2007). Out of order: Understanding repair and maintenance. *Theory, Culture & Society, 24*(3), 1–25.

The Greenbrier (2010).Welcome to the bunker [website]. Retrieved from: http://www.greenbrier.com/staying-here/the-bunker

Greenemeier, L. (2009, August 14). The great electric car quandary: How to build a charging infrastructure before demand grows. *Scientific American.* Retrieved from http://www.scientificamerican.com/article.cfm?id=electric-car-quandary

Gup, T. (1992, May 31). The ultimate congressional hideaway. *The Washington Post*, W11. Retrieved from http://www.washingtonpost.com/wp-srv/local/daily/july/25/brier1.htm

Halliday, J. (2010, September 24). Stuxnet worm is the 'work of a national government agency'. Guardian.co.uk. Retrieved from http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency

Halbert, D. (1997). Discourses of danger and the computer hacker. *Information Society, 13*(4), 361-374.

Harvey, D. (1989). *The condition of postmodernity*. Oxford: Blackwell.

Harvey, D. (1990). *Spaces of hope*. Berkeley: University of California Press.

Hay, J. (2001). Locating the televisual. *Television & New Media*, *2*(3), 205-234.

Hay, J. (2003). Unaided virtues: The (neo)liberalization of the domestic sphere and the new architecture of community. In J. Bratich, J. Packer, and C. McCarthy (Eds.), *Foucault, cultural studies, and governmentality*. Albany, NY: SUNY Press.

Hay, J. (2006). Designing homes to be the first line of defense. *Cultural Studies*, *20*(4/5), 349-377.

Hay, J. (2008). Outside media: Toward a study of watching ourselves through mobile media. *The Velvet Light Trap, 62,* 66-68.

Hay, J. & Andrejevic, M. (2006). Introduction. *Cultural Studies*, *20*(4/5), 331-348.

Hay, J. & Packer, J. (2004). Crossing the media (-N): Auto-mobility, the transported self and technologies of freedom. In N. Couldry and A. McCarthy (Eds.), *Mediaspace: Place, scale and culture in a media age* (pp. 209 – 232). London and New York: Routledge.

Healy, J. R. (2011, February 28). Feds postpone mandatory backup camera rule. *USA Today*. Retrieved from http://content.usatoday.com/communities/driveon/post/2011/02/feds-postpone-mandatory-backup-camera-rule/1

Hecht, J. (1999). *City of light: The story of fiber optics (revised and expanded edition).* Oxford and New York: Oxford University Press.

Hoyle, A. J. (2010, June 23). Raleigh's population soars past 400,000. *Triangle Business Journal*. Retrieved from http://www.bizjournals.com/triangle/stories/2010/06/21/daily17.html

Hsieh, M. (2009, September 3). Electromagnetic pulse discussion with Eric Hsieh. NEMAcast: The Electroindustry Podcast. Podcast retrieved from http://podcast.nema.org/index.php?id=14

Huler, S. (2010). *On the grid: A plot of land, an average neighborhood, and the systems that make our world work*. New York: Rodale.

Hughes, T. P. (1983). *Networks of power: Electrification in western society, 1880-1930*. Baltimore: Johns Hopkins University Press.

IBM (2011a). Instrumented. Intelligent. Interconnected. Retrieved from http://www.ibm.com/smarterplanet/us/en/overview/ideas/

IBM (2011b). Welcome to a smarter planet. Retrieved from http://www.ibm.com/smarterplanet/us/en/

Infrastructure. (2011). OED Online. Oxford University Press. Retrieved from http://www.oed.com.prox.lib.ncsu.edu/view/Entry/95624

Innis, H, A. (1951/2008). *The bias of communication* (2nd ed.). Toronto: University of Toronto Press.

Jackson, S., Edwards, P., Bowker, G., & Knobel, C. (2007, June). Understanding infrastructure: History, heuristics, and cyberinfrastructure policy. *First Monday, 12*(6).

Jansen, A. & Nielsen, R. (2005). Theorizing convergence: Co-evolution of information infrastructures. *Scandinavian Journal of Information Systems*, *17*(1), 67–100.

Jansson, A. & Falkheimer, J. (Eds.) (2006). *Geographies of communication: The spatial turn in media studies.* Göteborg, Sweden: NORDICOM.

Juhola, E., Stulberg, J. & Stulberg, R. (Producers) & Stulberg, J. & Stulberg, R. (Directors). (2007). *Off the Grid: Life on the Mesa* [Motion picture]. United States: Indiepix

Kaspersky Lab (2010, September 24). Kaspersky Lab provides its insights on Stuxnet worm. *Kaspersky Corporate News*. Retrieved from http://www.kaspersky.com/news?id=207576183

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., et al. (2010, May). Experimental security analysis of a modern automobile. Presented at the 2010 IEEE Symposium on Security and Privacy, Oakland, CA. Retrieved June 23, 2010, from http://www.autosec.org/pubs/cars-oakland2010.pdf

Latour, B. (1996). *Aramis: Or the love of technology*. Cambridge, MA and London: Harvard University Press.

Lefebvre, H. (1991). *The Production of space* (D. Nicholson-Smith, Trans.). Malden, MA: Blackwell Publishers (Original work published 1974).

Lewis, S. (September 22, 2008). The Etymology of infrastructure and the infrastructure of the internet [blog post]. *Hak Pak Sak: Stephen Lewis on Infrastructure, Identity, Communication, and Change.* Retrieved from http://hakpaksak.wordpress.com/2008/09/22/the-etymology-of-infrastructure-and-the-infrastructure-of-the-internet/

Maclean, W. (2010, September 24). UPDATE 2-Cyber attack appears to target Iran-tech firms. *Reuters*. Retrieved from http://www.reuters.com/article/idUSLDE68N1OI20100924

Markoff, J. (2010, September 26). A silent attack, but not a subtle one. *The New York Times.* Retrieved from http://www.nytimes.com/2010/09/27/technology/27virus.html?_r=1

Marx, L. (2000). *The machine in the garden: Technology and the pastoral ideal in America*. Oxford and New York: Oxford University Press.

McConnell, D. (2011, April 26). Iranian official: New computer worm discovered. *CNN Tech*. Retrieved from http://articles.cnn.com/2011-04-26/tech/iran.computer.worm_1_stuxnet-computer-worm-iranian-official?_s=PM:TECH

McMillan, R. (2010, September 14). Siemens: Stuxnet worm hit industrial systems. *PCWorld*. Retrieved from http://www.pcworld.com/businesscenter/article/205420/siemens_stuxnet_worm_hit_industrial_systems.html

Meadows, D. (2008). *Thinking in Systems: A Primer.* White River Junction, VT: Chelsea Green Publishing.

Merriman, P. (2007). *Driving spaces*. Malden, MA: Blackwell Publishing.

Milton, C. (2010, November 2). The "charge as you drive" electric car. *Clean Technica*. Retrieved from http://cleantechnica.com/2010/11/02/the-charge-as-you-drive-electric-car/

Moteff, J. & Parfomak, P. (2004, September 1). Critical infrastructure and key assets: Definition and identification (Congressional Report No. RL32631). Washington DC: Library of Congress Congressional Research Service. Retrieved from Federation of American Scientists website: http://www.fas.org/sgp/crs/RL32631.pdf

Moyer, M. (2010, June 22). The dirty truth about plug-in hybrids: How green is that electric car? Depends on where you plug it in. *Scientific American.* Retrieved from http://www.scientificamerican.com/article.cfm?id=the-dirty-truth-about-plug-in-hybrids

Moyer, M (2010, October 26). Window shopping for electric cars: How to compare conventional and plug-in vehicles. *Scientific American.* Retrieved from http://www.scientificamerican.com/article.cfm?id=window-shopping-for-electric-cars

National Energy Education Development Project (2005). H2 Educate Student Guide (2011). Retrieved from http://www.need.org/needpdf/H2%20Educate%20Student%20Guide.pdf

National Highway Traffic Safety Administration (2009). Consumer Assistance to Recycle and Save Act of 2009. Report to the House Committee on Energy and Commerce, the Senate Committee on Commerce, Science, and Transportation and the House and Senate Committees on Appropriations. Retrieved from http://www.cars.gov/files/official-information/CARS-Report-to-Congress.pdf

National Highway Transportation Safety Administration (2010, December 3). U.S. DOT Proposes Rear View Visibility Rule to Protect Kids and the Elderly [press release]. Retrieved from http://www.nhtsa.gov/PR/NHTSA-17-10

Nissan (2011). The new car: features and specifications [website]. Retrieved from http://www.nissanusa.com/leaf-electric-car/

No Author (1921). How can mass transport remain a monopoly? *Electric Railway Journal 58*(9) 305-306. Retrieved from http://www.archive.org/stream/electricrailwayj581mcgrrich#page/14/mode/2up

No Author (1915). Traffic and transport: The jitney bus. *Electric Railway Journal 45*(23) 1092-1094. Retrieved from http://www.archive.org/stream/electricrailwayj4546mcgrrich#page/1092/mode/2up

No Author (1916). The vehicular traffic menace. *Electric Railway Journal 48*(18) 917-918. Retrieved from http://www.archive.org/stream/electricrailwayj482mcgrrich#page/24/mode/2up

NPR Staff (2011, March 26). The secret bunker congress never used. *All Things Considered*. Retrieved from http://www.npr.org/2011/03/26/134379296/the-secret-bunker-congress-never-used

"Observer" (1921). Des Moines rides busses and walks. *Electric Railway Journal 58*(8) 283-288. Retrieved from http://www.archive.org/stream/electricrailwayj581mcgrrich#page/282/mode/2up

O'Murchu, L. (2010). Last-minute paper: An indepth look into Stuxnet [abstract]. Virus Bulletin International Conference, September 29 – October 1 2010, Vancouver, BC, Canada. Retrieved from http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml

Ordinance. (2011). OED Online. Oxford University Press. Retrieved from http://www.oed.com.prox.lib.ncsu.edu/view/Entry/132352

Ordnance. (2011). OED Online. Oxford University Press. Retrieved from http://www.oed.com.prox.lib.ncsu.edu/view/Entry/132370

Oswald, K. F. & Packer, J. (2011). Flow and mobile media: Broadcast fixity to digital fluidity. In J. Packer and S. Wiley (Eds.) *Communication Matters: Materialist Approaches to Media, Mobility, and Networks.* London: Routledge.

Packer, J. (2002). Mobile communications and governing the mobile: CBs and truckers. *The Communication Review*, *5*, 39–57.

Packer, J. (2006). Rethinking dependency: New relations of transportation and communication. In J. Packer & C. Robertson (Eds.) *Thinking with James Carey: Essays on communications, transportation, history* (pp. 79-99). New York: Peter Lang

Packer, J. (2007). Auto militarization: Citizen soldiers, the Hummer, and the War on Terror. In E. Cardenas and E. Gorman (Eds.), *The Hummer: Myths and consumer culture* (pp. 207-219). Lanham, MD: Lexington Books.

Packer, J. (2008). *Mobility without mayhem*. Durham, NC: Duke University Press.

Packer, J. (2010). What is an archive?: An apparatus model for communications and media history. *The Communication Review*, *12*(1), 88-104

Packer, J. & Oswald, K. F. (2010). From windscreen to widescreen: Screening technologies and mobile communication. *The Communication Review*, *13*(4) 309-339.

Packer, J., & Wiley, S.B.C. (Eds.) (2011). *Communication matters: Media, mobility, and networks*. London: Routledge.

Parks, L. (2004). Kinetic screens: Epistemologies of movement at the interface. In N. Couldry and A. McCarthy (Eds.) *Media/Space: Place, scale and culture in a media age* (pp. 37-57). London: Routledge.

Pricewaterhouse Coopers (2009, July 27). The future's electric for auto industry but barriers may short circuit the sparks, says PricewaterhouseCoopers [Press Release]. Retrieved from http://www.pwc.com/gx/en/press-room/2009/future-electric-for-auto-industry.jhtml

Pontius, D. W. (1923). Co-ordination of trolley and bus in California. *Electric Railway Journal*, *62*(15) 597-599. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/596/mode/2up

Presidential Decision Directive 63 (1998). Retrieved from Federation of American Scientists Presidential Directives and Executive Orders Database: http://www.fas.org

Rahim, S. and Climatewire (2010, October 4). How automakers can meet new fuel efficiency standards. *Scientific American*. Retrieved from http://www.scientificamerican.com/article.cfm?id=how-automakers-can-meet-new-fuel

Ramsey, M. (2010, September 1). General Motors wants trademark for 'Range Anxiety'. *Driver's Seat: The Wall Street Journal* [weblog]. Retrieved from http://blogs.wsj.com/drivers-seat/2010/09/01/general-motors-wants-trademark-for-range-anxiety/

Ratliff, E. (2009). Gone: What does it take to really disappear? *Wired 17.09*, 120-126; 140.

Renewable Fuels Association (2011a). Market opportunities: Fuel cells [website]. Retrieved from http://www.ethanolrfa.org/pages/fuel-cells

Renewable Fuels Association (2011b). Statistics [website]. Retrieved from http://www.ethanolrfa.org/pages/statistics

Romero, F. (2009, January 13). A brief history of the electric car. *Time.com*. Retrieved from http://www.time.com/time/business/article/0,8599,1871282,00.html

Romm, J. J. (2004). *The hype about hydrogen: Fact and fiction in the race to save the climate*. Washington, DC: Island Press.

Rosen, N. (2010). *Off the grid: Inside the movement for more space, less government, and true independence in modern America*. USA: Penguin Group.

Russill, C. (2008). Sublimity and solutions: Problematization in ICT for development perspectives. *Communication and Critical/Cultural Studies, 5*(4) 383-403.

Salvatore, R. D. (2006). Imperial mechanics: South America's hemispheric integration in the Machine Age. *American Quarterly, 58*(3), 662-691.

Schewe, P. (2006). *The grid: A journey through the heart of our electrified world*. Washington D.C.: Joseph Henry Press.

Schivelbusch, W. (1977/1986). The railway journey: The industrialization of time and space in the 19th century. Berkeley and Los Angeles: University of California Press.

Sheller, M. (2007). Bodies, cybercars and the mundane incorporation of automated mobilities. *Social & Cultural Geography, 8*, 175–197.

Sherwood, B. (2009). *The survivors club: The secrets and science that could save your life*. New York: Grand Central Publishing.

Slack, J. D. & Wise, J. M. (2005). *Culture and technology: a Primer*. New York: Peter Lang

Soja, E. J. (1996). *Thirdspace: Journeys to Los Angeles and other real-and-imagined places*. Malden, MA: Blackwell.

Sophos (2010). Security threat report: 2010. Retrieved from http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-jan-2010-wpna.pdf

de Souza e Silva, A. & Frith, J. (2010). A critical analysis of locative social mobile networks: Merging communication, location and urban spaces. *Mobilities*, *5*(4): 485-505.

de Souza e Silva, A. & Sutko, D. M. (2009). *Digital cityscapes: Merging digital and urban playspaces*. New York: Peter Lang.

Spigel, L. (2001). Media homes: Then and now. *International Journal of Cultural Studies, 4*(4), 385-411.

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist, 43*, 377-391.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111-133.

Stocks, C. W. (1930). Improving the bus to increase its usefulness. *Electric Railway Journal, 74*(7) 387-390. Retrieved from http://www.archive.org/stream/electricrailwayj742mcgrrich#page/386/mode/2up

Stored Communications Act (SCA) of 1986. 18 U.S.C. §§ 2701 to 2712.

Storrs, L. S. (1923). Adding the bus to existing facilities. *Electric Railway Journal, 62*(15) 589-590. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/588/mode/2up

Streeter, T. (1996). *Selling the air: A critique of the policy of commercial broadcasting in the United States*. Chicago: University of Chicago Press.

Sullivan, C. (2009, March 10). California planning for alternative fuel highway. *Scientific American Greenwire.* Retrieved from http://www.scientificamerican.com/article.cfm?id=alternative-energy-fuel-highway

Sulzberger, C. (2004). An early road warrior: Electric vehicles in the early years of the automobile. *IEEE Power Engineering Society.* Retrieved from http://www.ieee.org/organizations/pes/public/2004/may/peshistory.html

Survival Condo (2011) Survivalcondo.com [website]. Retrieved from http://www.survivalcondo.com/

System. (2011). OED Online. Oxford University Press. Retrieved from http://www.oed.com.prox.lib.ncsu.edu/view/Entry/196665

Taylor, G. R. (1951/1966). *The transportation revolution 1815-1860.* Armonk, NY: M. E. Sharpe, Inc.

Taylor, P. A. (2001). Informational intimacy and futuristic flu: Love and confusion in the matrix. *Information Communication & Society, 4*(1), 74-94.

Tesla Motors (2011). Roadster specs [website]. Retrieved from http://www.teslamotors.com/roadster/specs

Theohary, C. A., & Rollins, J. (2009, September 30). Cybersecurity: Current legislation, executive branch initiative, and options for Congress (Congressional Report No. R40836). Washington DC: Library of Congress Congressional Research Service. Retrieved from Open CRS website: http://assets.opencrs.com/rpts/R40836_20090930.pdf

U.S. Department of Labor, Bureau of Labor Statistics (2011). Occupational outlook handbook, 2010-11 Edition, automotive service technicians and mechanics. Retrieved from http://www.bls.gov/oco/ocos181.htm

U.S. Census Bureau (2009a). Retail trade: Industry series: Preliminary summary statistics for the United States: 2007. [Table]. Retrieved from http://factfinder.census.gov/servlet/IBQTable?_bm=y&-geo_id=&-ds_name=EC0744I1&-_lang=en

U.S. Census Bureau (2009b). Sector 81: EC0781I1: Other services (except public administration): Industry series: Preliminary summary statistics for the United States: 2007. [Table]. Retrieved from http://factfinder.census.gov/servlet/IBQTable?_bm=y&-geo_id=&-ds_name=EC0781I1&-_lang=en

U.S. Department of Homeland Security (November 30, 2010a). Critical infrastructure [website]. Retrieved from http://www.dhs.gov/files/programs/gc_1189168948944.shtm

U. S. Department of Homeland Security (2010b). Communications Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. Retrieved from http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf

U. S. Department of Homeland Security (2010c) National Infrastructure Protection Plan: Communications Sector. Retrieved from http://www.dhs.gov/xlibrary/assets/nipp_snapshot_communications.pdf

U. S. Department of Justice (2004). Report from the field: USA PATRIOT Act at work. Retrieved from http://www.justice.gov/olp/pdf/patriot_report_from_the_field0704.pdf

U. S. Department of Transportation (2010). Fiscal year 2011 budget highlights. Retrieved from http://www.dot.gov/budget/2011/2011budgethighlights.pdf

U.S. Energy Information Administration (2011a). Monthly energy review. Petroleum consumption: Transportation and electric power sectors [Table 3.7c]. Retrieved from http://www.eia.gov/totalenergy/data/monthly/pdf/sec3_21.pdf

U. S. Energy Information Administration (2011b). Oil: Crude and petroleum products *Explained*. Retrieved from http://www.eia.doe.gov/energyexplained/index.cfm?page=oil_home#tab2

U. S. Energy Information Administration (2011c). Net generation by energy source: Total (all sectors) [Table]. Retrieved from http://www.eia.doe.gov/cneaf/electricity/epm/table1_1.html

U. S. Energy Information Administration (2011d). Petroleum and other liquids. Weekly United States spot price FOB weighted by estimated import volume (dollars per barrel) [Table]. Retrieved from http://www.eia.gov/dnav/pet/hist/LeafHandler.ashx?n=PET&s=EMM_EPM0_PTE_NUS_DPG&f=W

U. S. Environmental Protection Agency (2009). Supporting statement for OMB review of EPA ICR No. 2362.01: Information collection request for National Emission Standards for Hazardous Air Pollutants (NESHAP) for coal- and oil-fired electric utility steam generating units; Part B (EPA-HQ-OAR-2009-0234-0002.1). Retrieved from regulations.gov database: http://www.regulations.gov/#!documentDetail;D=EPA-HQ-OAR-2009-0234-0002.1

U. S. Federal Emergency Management Agency (2004). *Are you ready?* [White paper]. Retrieved from http://www.fema.gov/areyouready/index.shtm

U. S. Federal Emergency Management Agency (1980). Home Fallout Shelter snack bar basement location plan d. Retrieved from http://www.archive.org/details/HomeFalloutShelterSnackBarBasementLocationPlanD

U. S. Research and Innovative Technology Administration (2010a). Number of U.S. aircraft, vehicles, vessels, and other conveyances, Table 1-11. Retrieved from http://www.bts.gov/publications/national_transportation_statistics/html/table_01_11.html

U. S. Research and Innovative Technology Administration (2010b). System mileage within the United States, Table 1-11. Retrieved from http://www.bts.gov/publications/national_transportation_statistics/html/table_01_11.html

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107 –56. 115 Stat. 272 (2001). Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

University of Groningen Website (n.d.). *Sibrandus Stratingh (1785-1841): Professor of Chemistry and Technology*. Retrieved from http://www.rug.nl/museum/geschiedenis/hoogleraren/stratingh?lang=en

Urry, J. (2007). *Mobilities*. Cambridge and Malden, MA: Polity Press.

Urry, J. (2003). Social networks, travel and talk. *British Journal of Sociology, 54*(2), 155-175.

Ventura, J. (Host). (2010, January 13). Apocolypse 2012 [Television series episode]. In R. Acutt, J. Sarpong & J. Ventura (producers) *Conspiracy Theory with Jesse Ventura*. Los Angeles: A. Smith & Co. Productions.

Virilio, P. (1975/1994). *Bunker archeology*. New York: Princeton Architectural Press.

Vivos Group (2009). *Surviving economic anarchy* [white paper]. Retrieved from http://www.terravivos.com/images/SurvivingEconomicAnarchy.pdf

Vivos Group (2010). *Survivalist versus survivor: Vivos is not about "survivalist", but rather surviving* [white paper]. Retrieved from http://www.terravivos.com/images/survivalistpaper.pdf

Vivos Group (2011). Vivos threat scenarios. Retrieved from http://www.terravivos.com/secure/threatscenarios.htm

Vivos Group (2011). Chosen. Retrieved from http://www.terravivos.com/secure/chosen.htm

Vivos Group (2011). Will you survive in a backyard shelter?. Retrieved from http://www.terravivos.com/secure/backyard.htm

Vivos Group (2011). Vivos gold standard. Retrieved from http://www.terravivos.com/secure/goldstandard.htm

Walsh, B. (2008, November 3). The top 10 of everything 2008: A yearbook of all the top events you've been talking about: Ethanol bubble bursts. *Time*. Retrieved from http://www.time.com/time/specials/packages/article/0,28804,1855948_1863706_1863712,00.html

Warrick, J. (2011, February 16). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021506501.html

Wellman, B., Hogan, B., Berg, K., et al (2005) Connected lives: The project, in P. Purcell (Ed.) *Networked Neighbourhoods* (pp. 1-50). Berlin: Springer.

Welsh, J. W. (1923). American Association Proceedings. Published in the *Electric Railway Journal, 62*(15) 616 - 632. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/616/mode/2up

Weintraub, A., & Kerstetter, J. (2003, June 9). Cyber alert: Portrait of an ex-hacker. *Business Week*, p.116.

White Busses (September 29, 1923). Moving people has become the twin problem of moving materials. *Electric Railway Journal 62* 120-121. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/n535/mode/2up

The White House, Office of the Press Secretary (2009). Remarks by the President on Securing our Nation's Cyber Infrastructure [Press release]. Retrieved from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/

Wiener, N. (1965). *Cybernetics: Or control and communication in the animal and the machine*. Cambridge, MA: MIT Press

Wiley, S. B.C. (2004). Rethinking nationality in global context. *Communication Theory 14*(1), 78-96.

Wiley, S. B. C. (2005). Spatial materialism: Grossberg's Deleuzean cultural studies. *Cultural Studies, 19*(1), 63-99.

Wiley, S.B.C., Moreno, T. & Sutko, D.M., (2010). Assemblages, networks, subjects: A materialist approach to the production of social space. In J. Packer and S. Wiley (Eds.) *Communication Matters: Materialist Approaches to Media, Mobility, and Networks.* London: Routledge.

Wiley, S.B.C., Sutko, D.M., and Moreno, T. (2010). Assembling social space. *The Communication Review*, *13*(4), 340-372.

Williams, R. (2003). *Television: Technology and cultural form*. New York: Routledge. (Originally published 1974).

Winner, L. (1986). *The Whale and the reactor: A search for limits in an age of high technology*. Chicago: University of Chicago Press.

Winsor, H. G. (1916). Motor vehicle accidents and traffic regulation. *Electric Railway Journal 48*(17) 874-876. Retrieved from http://www.archive.org/stream/electricrailwayj482mcgrrich#page/874/mode/2up

Wynne, L. F. (1923, October 20). Psychology of the automobilist. *Electric Railway Journal 62*(16) 689-690. Retrieved from http://www.archive.org/stream/electricrailwayj622mcgrrich#page/688/mode/2up

Yellow Coach (1930, May). [Advertisement]. *Electric Railway Journal* page 34-37. Retrieved from http://www.archive.org/stream/electricrailwayj742mcgrrich#page/n103/mode/2up

Young, G. & Meyers, T. (2010, July 23). Cable cars, trolleys and monorails. *Bowrey Boys Podcast* retrieved from http://boweryboys.libsyn.com/_107_new_york_s_elevated_railroads

Zetter, K. (2010, September 23). Blockbuster worm aimed for infrastructure, but no proof Iran nukes were target. *Wired.com: Threat Level: Privacy, Crime, and Security Online*. Retrieved from http://www.wired.com/threatlevel/2010/09/stuxnet/