Fall 12-2017

Sony Pictures and the U.S. Federal Government: A Case Study Analysis of the Sony Pictures Entertainment Hack Crisis Using Normal Accidents Theory

Mohamed Ismail
University of Southern Mississippi

SONY PICTURES AND THE U.S. FEDERAL GOVERNMENT: A CASE STUDY ANALYSIS OF THE SONY PICTURES ENTERTAINMENT HACK CRISIS USING NORMAL ACCIDENTS THEORY

by

Mohamed Ismail

A Thesis
Submitted to the Graduate School,
the College of Arts and Letters,
and the Department of Communication Studies
at The University of Southern Mississippi
in Partial Fulfillment of the Requirements
for the Degree of Master of Arts

December 2017

SONY PICTURES AND THE U.S. FEDERAL GOVERNMENT: A CASE STUDY ANALYSIS OF THE SONY PICTURES ENTERTAINMENT HACK CRISIS USING NORMAL ACCIDENTS THEORY

by Mohamed Ismail

December 2017

Approved by:

_____
Dr. Steven Venette, Committee Chair
Professor, Communication Studies

_____
Dr. John Meyer, Committee Member
Professor, Communication Studies

_____
Dr. Kathryn Anthony, Committee Member
Assistant Professor, Communication Studies

_____
Dr. Wendy Atkins-Sayre
Chair, Department of Communication Studies

_____
Dr. Karen S. Coats
Dean of the Graduate School

Published by the Graduate School

ABSTRACT

SONY PICTURES AND THE U.S. FEDERAL GOVERNMENT: A CASE STUDY ANALYSIS OF THE SONY PICTURES ENTERTAINMENT HACK CRISIS USING NORMAL ACCIDENTS THEORY

by Mohamed Ismail

December2017

In this case study, I analyze the 2014 North Korean computer database hack of Sony Pictures Entertainment (SPE), a serious national security crisis of cyberterrorism. I utilize Normal Accidents theory as a lens, to help explain how the accident within one system (SPE) and later crisis lead to the interaction with a second system (U.S. Federal Government), the development of a new crisis, and the need for a crisis response from system two. The evolution of a single organization's accident into a national security crisis does not occur without specific complex interactions that take place to connect the two systems together. To explain this interconnectedness between systems, I introduce two new constructs: 1) common denominator and 2) common goal, which expand Normal Accidents theory allowing it to account for the coupling between the two independent systems (SPE & United States Government) through non-linear interactions. Overall, this case study provides important insight for future crisis communication planning, response, and development regarding between-organization interaction during a crisis.

ACKNOWLEDGEMENTS

I would like to thank my university and department, the University of Southern Mississippi and Department of Communication Studies for providing me with a platform to grow as a scholar over the years. I am proud to have completed this project and my graduate studies here.

Thank you to my advisor, Dr. Steven Venette for being there to guide me throughout this project. From day one in our crisis communication class when I first proposed this research to you as a class paper you have always been supportive and empowering. It has been a great pleasure to learn from you, work alongside you, and receive your assistance, insight, and encouragement throughout this project, and I thank you greatly. Also, I would like to thank my committee members Dr. Kathryn Anthony and Dr. John Meyer for all their feedback and guidance during this project that boosted me to develop an overall stronger piece.

A special thanks to Dr. Wendy Atkins-Sayre for shaping my graduate school trajectory and experience. You have always been an endless source of genuine and caring support throughout the entirety of my graduate tenure and I appreciate it more than you will ever know. Moreover, thank you for providing me the opportunity to work for you in the USM Speaking Center. Without being a Speaking Center graduate tutor I do not believe my graduate school experience would have been as fulfilling and liberating as it has been. That opportunity alone I hold immensely dear, thank you.

Dr. Keith Erickson, even when I was a sophomore in your Introduction to Public Speaking course you saw in me a communication scholar that I never knew existed. I remember vividly after my speech your feedback notes saying, “you should be a comm

student" and here I am now. Your wisdom, mentorship, and friendship from that day forward was the catalyst for why I pursued my graduate degree in Communication Studies, and I cannot express my gratitude to you enough.

Thank you to all my friends for your endless camaraderie. Each of you in your own way gave me so much life and joy amidst the various responsibilities that accompanied graduate school. A special thanks to my dear friends and colleagues, Tori Brown and Carley Reynolds. You two are the one and two to our three musketeers. Thank you for being such loyal, caring, present, and giving friends. From being together during tough academic endeavors to our late-night laughs and drives, I am blessed to have met you through scholarship and have you as my friends for life.

Finally, and with my entire heart, soul, and being I thank you, my beautiful wife – Olivia Ismail, my lovely mother – Dr. Nagwa Megahed, my brilliant father – Mohi Ismail, and my wonderful brother – Ahmed Ismail. There are no words that can truly explain how thankful I am for all of you, but here goes.

Olivia, زوجتي, the definition of altruism holds no meaning without your existence. Every single step of the way, even when I did not want to take anymore, you were by my side with unconditional love and unwavering support. During this project from its inception to its final sentence, you made sure I stayed the course and successfully finished what I began. You were my coach, my cheerleader, my team, and everything in between, and without you this project would not be complete. Habibty, I thank you for everything that you are and all that you have been for me in life and throughout this process. These feelings won't go away. I love you!

Mom, أمي, it is my absolute honor to be your son, the son of the greatest professor ever – YOU! I was 10 years old when I watched you walk across the stage at the University of Pitt to receive your PhD, a triumphant moment engrained in my memory forever and a guiding light for where I am today. You are the most outstanding scholar and mother, and I am beyond lucky to have both all-in-one! Whether it was to check up on me and make sure I was okay or guide me through every academic project since elementary school including this one, you have been my mentor, my advisor, and my role model. You are the sun to my garden that has helped me grow abundantly. I love you!

Dad, ابي, the depths of the ocean are unmatched to the depths of your wisdom and care. It is my greatest privilege to be your son. The road to finishing this thesis was like the cobblestone road you taught me to ride my bike on – hard and unsteady at times. And just like on the bike, I fell a few times. Yet, just like you did back then when I was scared to get back on and try again, you made sure I pedaled my way strong to the end of this project. I love you!

Ahmed, اخي, as I have said countless times before: you inspire me! You motivate me, and because of you I always challenge myself in aim of being the best role model for you, whether as a scholar or brother. Throughout this project, I remember calling you on many occasions to talk or just vent to you, and you listening intently in godly support. You provided me with perspective way beyond your years that rejuvenated my soul and gave me strength to continue my pursuit. I love you!

In close, alone in this endeavor, I was never. To all, I thank you kindly.

DEDICATION

To my wife, mother, father, and brother.

The greatest part of my life.

Shokran.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

SPE	Sony Pictures Entertainment
GOP	Guardians of the Peace
USM	University of Southern Mississippi

CHAPTER I - INTRODUCTION

The 2014 North Korean computer database hack of Sony Pictures Entertainment (SPE) stormed to the forefront of the nation's attention as not just a great piece of celebrity news, but as a serious national security crisis of cyberterrorism. This cyber terrorist attack in its early stages was presumed to be a hoax. However, as it transpired and email threats were followed through by action it became evident that this was indeed a crisis that needed national security intervention.

Many Americans are familiar with the concept of terrorism, and upon hearing the word can automatically conjure a specific mental picture in connection (Hermann, 1984). The American Civil Code defines terrorism as "premeditated violence, politically motivated against civilians, committed by local groups or clandestine agents, in order to influence a target audience" (American Civil Code, as quoted by Paul, Bugnar, & Mester, 2015, p. 7). However, in this technological age terrorism can extend beyond our physical world in forms that surpass the generic "violence" as noted in the above definition, and this extension is known as cyberterrorism. "Cyberterrorism means premeditated, politically motivated attacks by sub national groups, clandestine agents, or individuals against information and computer systems, computer programs, and data that result in violence against non-combatant targets" (Janczewski, 2007, xii). In turn, rather than a physical act of terror cyberterrorism transforms terrorism to a virtual attack that is boundless through an Internet world.

Cyberterrorism has proven to be of major concern for various reasons (e.g., privacy, security, economics, and freedom) organizationally, nationally, and internationally (Atalay & Sanci, 2015; Yong-joon, Hyuk-jin, Jaeil, & Dong-kyoo, 2015).

Currently, with the social and financial lives of individuals being readily available and accessible on the Internet, it allows for easier connectivity and takeover of that which people hold valuable (Matusitz, 2014). The unsettling aspect of cyberterrorism is its ability to take on any form to ruin its target; the spread of incorrect information, the collapse of a computer system, and information altering are just a few of the methods used via cyberterrorism to affect the target population (Kennedy, 2001; Matusitz, 2014; Weimann, 2005).

The SPE hack serves as an act of cyberterrorism because the hackers – "Guardians of Peace" – were later identified as a national Korean group (The White House, 2015a). This group used this hack as a politically motivated attack against SPE's computer system to stop SPE from releasing its film – *The Interview*, which satirically depicted the North Korean Supreme Leader, Kim Jong Un. This act of cyberterrorism later transformed into a national security crisis once it negatively impacted American values (freedom of speech), shut down a major non-combatant organization's (SPE) system, and destroyed certain private information of American citizens (SPE Employees). Ultimately, the SPE hack is an exemplar of a crisis catalyzed through cyberterrorism as it took control of a major corporation's system via Internet connectivity, and consequently shocked a nation's sense of security and normalcy.

However, crises are not "one-size-fits-all" but vary in type and intensity (Seeger, Sellnow, & Ulmer, 2003). Generally, a 'crisis' is an "unusual event of overwhelmingly negative significance that carries a high level of risk, harm, and opportunity for further loss (Seeger et al., 2003, p. 3). Nonetheless, in Heath and O'Hair's (2010) risk and crisis communication handbook and Coombs and Holladay's (2011) handbook on crisis

communication they define crisis and crisis communication, and provide Coombs' inclusive and holistic definition of crisis:

> A crisis can be viewed as the perception of an event that threatens important expectancies of stakeholders and can impact the organization's performance. Crises are largely perceptual. If stakeholders believe there is a crisis, the organization is in a crisis unless it can successfully persuade stakeholders it is not. A crisis violates expectations; an organization has done something stakeholders feel is inappropriate. (Coombs, 2009, p. 100)

Based on the definition of crisis, the SPE hack is a more focused form of crisis, and can be identified as an organizational crisis – "a specific unexpected and non-routine organizationally based event or series of events which creates high levels of uncertainty and threat or perceived threat to an organization's high priority goals" (Seeger, Sellnow, & Ulmer, 1998, p. 233) that was induced by an act of cyber terrorism.

Significance

Crisis communication literature has looked at various organizational crises to study each organization's mode of operation pre-crisis, during crisis, and post crisis (see: Benoit, 1995; Coombs, 1999; Seeger, 2006; and Seeger, et al., 2003). Seeger (2006) notes that there exists various crisis types and different dynamics within each crisis that prompts crisis communication scholars to develop adequate strategies to address these variances in crises. The Sony Pictures crisis is a unique case to study as it includes the interconnectedness of two separate organizations, a private company – SPE – with a public entity – U.S. Federal government – in response to a crisis. Therefore, it serves as a novel organizational crisis to analyze for crisis strategy development. More importantly,

this study is unique in that it uses Normal Accidents theory to better understand these complex interactions between systems during a high stress crisis event. A between systems crisis is when the crisis of one organization directly impacts a second organization. In this case, the initial interaction is between Sony Pictures Entertainment and the United States Federal Government; which later lead to a national security crisis between the U.S. and North Korea.

Existing literature studying the interaction between two separate organizations in response to the crisis of one does not explore this phenomenon using Normal Accidents theory as its central point of analysis (See: Gotham, 2012; Millner, 2011; and Millner, Veil, & Sellnow, 2011). Millner et al. (2011) highlights how third party organizations within affiliated industries serve as proxy communicators in resolution of a crisis when the main organization fails to appropriately respond. Gotham (2012) notes that the implementation of policy from certain organizations (e.g., financial firms) can develop problems in other organizations (e.g., mortgage market) and later lead to full-blown crisis (e.g., 2007 U.S. financial housing crisis) via a cascading effect (i.e., Crisis-Policy Nexus). However, these studies do not indicate how two varying systems interact through the sharing of each other's subsystems in response to the initial accident and later against the unfolding of a new crisis.

Additionally, the existing literature does not highlight the interaction between a private organization and a public entity, as shown in this case. Liu, Horsley, and Levenshus (2010) identify the differences and similarities between government entities and private sectors. However, these findings only indicate how the private and public sector would individually communicate given the potential emergence of a situation. The

study does not assess a “real-life” case where the two organizations interact and their communication intersects in response to a specific happening. This current study does. Thus, an analysis of the Sony Pictures hack crisis and its interaction with the U.S. Federal government is of significance for communication scholars to better understand using Normal Accidents theory as the underpinning that facilitates the interaction of these two separate types of organizations during a crisis.

This evolution of a single organization’s crisis into a national security crisis does not occur without specific communicative interactions that occur to connect organizations together. Communication scholars have developed a plethora of research on the role communication plays within organizational crises and the best practices for organizational crisis management (Seeger, 2006). Coombs (2010) states that, "the reality of crises leads to the need for preparation and readiness to respond – crisis management. The critical component in crisis management is communication” (p. 17). Previous research on crisis communication has primarily focused on crisis prevention and management within one organization, but has fallen short in identifying strategies that assist when one crisis effects two organizations of varying make-up simultaneously. Therefore, it is essential to further expand the existing research on best practices and communicative crisis management strategies to assist organizations in crises that involve between-organization interaction.

In this paper, I uncover the role communication plays in between-organization interaction during a crisis. I use Normal Accidents theory as the guiding theoretical framework to analyze the case. Normal Accidents theory has only accounted for accidents that manifest within one system. In turn, this study expands Normal Accidents

theory's reach allowing it to explain complex interactions between two systems. Furthermore, I use an explanatory case study approach with descriptive analysis to understand how the Sony Pictures hack became an organizational crisis, and why it interacted with the U.S. Federal Government to then create a national security crisis.

Current crisis communication case study research usually focuses on a single crisis and how it impacts the one organization's operation (see: Venette, Sellnow, & Lang, 2003). These case studies are used to highlight both the successes and failures of organizations when managing their crises. In turn, researchers take these various case study findings and develop a foundation of advice for future organizations regarding their crisis plan (Coombs, 2010).

Using the case study approach, I identify how these two organizations interacted with one another during a crisis. This extends the case study method within crisis communication to include the analysis of interconnected crises that impact system wide operations across multiple organizations from a Normal Accidents theory perspective. It reveals how the failure of one organization (SPE) due to cyberterrorism negatively impacts a second organization (United States Government) to create a greater independent crisis – national security threat between the United States and North Korea.

Overview of Chapters

This study is arranged into the following chapters. Chapter two provides a review of literature focusing on Normal Accidents theory and complex organizations. Chapter three presents an overview of the methodological approach utilized – explanatory case study with descriptive analysis under a single case study design. In it, I justify why case study analysis was the qualitative method of choice for this research; I highlight how the

data was collected; and finally, I discuss how the data was analyzed. Chapter four provides detailed information regarding the SPE hack crisis case and stitches together its evolution and transformation throughout the progression of the crisis using a timeline narrative approach. Finally, chapter five discusses the pertinent conclusions of this research project. Moreover, chapter five highlights implications, limitations, and future research opportunities. The next chapter reviews literature applicable to this research.

CHAPTER II - LITERATURE REVIEW

Theoretical Framework: Normal Accidents Theory

When crises occur, they are usually catalyzed via a specific occurrence that disrupts the state of operational normalcy in an organization (Perrow 1999; and Seeger 2002). Crisis communication aims to establish proactive, pre-crisis, means against this disruptive occurrence from ever happening. This proactive intervention can only be established through a breadth of understanding related to the organizational make-up where the crisis can take place (Coombs, 2014).

Charles Perrow (1999) argues that as human development continues to expand through technology, political agendas, and globalization systems are created to account and manage for this expansion, specifically technologically advanced systems. Systems, as Perrow (1999) points, are organizations, and these systems in and of themselves contain subsystems that constitute the organization's internal infrastructure (from this point forward 'systems' and 'organizations' will be used interchangeably). These systems continue to grow in intricacy and complexity, which increases their "riskiness" and in succession makes them predisposed to being of catastrophic potential. However, Perrow (1999) argues that because of this increased complexity within systems these disruptive occurrences become "normal accidents" that are inevitable due to the innate high-risk nature of these organizations. An 'accident' is an unintentional occurrence that disrupts normalcy by causing damage to people, objects, or both (Coombs & Holladay, 1996; Perrow, 1999; Seeger 2002; and Seeger, Sellnow, & Ulmer, 2003). Thus, "if we can understand the nature of risky enterprises better we may be able to reduce or even remove these dangers" (Perrow, 1999, p. 3). More importantly, if accidents in increasingly

complex systems are normal and in turn inevitable, we as communication scholars must identify means to address these accidents as an extension of the organization's normalcy without allowing them to manifest into crises.

Perrow (1999), through analysis of various high-risk system accidents, developed Normal Accidents Theory, a theory that explains how organizational crises of catastrophic consequences occur via accidents within systems due to their interactive complexity. In this section, I explain the major concepts of Normal Accidents theory, and justify why it is an appropriate and strong theoretical framework to analyze the Sony Pictures hack crisis.

Perrow (1999) identifies that systems that are prone to these normal accidents are 'complex' systems; meaning, they are systems that consist of a multitude of variables that could find themselves interconnected with one another out of sequence. These complex systems differ greatly to their counterpart, linear systems, seeing as they do not operate in a sequential (e.g., conveyer belt) mode of operation (Perrow, 2011). Linear systems are identified as simple systems, compared to complex systems, as they can easily substitute or replace any supplies and equipment during the occurrence of an accident, due to their extensive availability. They accomplish this because of their "assembly line-like" operational design. This allows for ease of maintenance and minimal disturbance to the remainder of the system if a crisis were to occur during a malfunction of one component. The variables in complex systems are known as subsystems - multiple moving parts within the system that individually play a significant role to produce the overall system's final product. These subsystems can also be interdependent to where the malfunction of one has the potential to impact the status of the other. Therefore, complex systems are

usually referred to as ‘high-risk’ systems (e.g. chemical plants, aircraft carriers, and nuclear plants).

These high-risk systems are complex because they consist of specialized personnel and subsystems that are highly interactive with one another to accomplish their system’s agenda (Perrow, 1967; 1984; 1999; and 2011). Although, complex systems contain highly interactive subsystems, ‘complex interactions’ are usually “unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible” (Perrow, 1999, p. 78). They are complex interactions because they occur outside of the organization’s normal production sequence between two subsystems that are known to be unrelated in the system’s original design and operation.

Thus, understanding the composition of a complex system and how it operates, and the potentiality of complex interactions grants communication scholars a stronger grasp on how to better diagnose a crisis that could happen within a similar organization. As noted by Coombs and Holladay (1996), “characteristics of the crisis situation should suggest to the crisis manager the best crisis response strategy or strategies to fit the situation” (p. 284). For example, the accident at the Three Mile Island nuclear plant in 1978 highlighted how the malfunction of one subsystem (condensate polisher) impacted the malfunction of another subsystem (feed water pumps), and finally the failure of the major subsystem (pilot-operated relief valve); which ultimately lead to the release of radioactive gases into the environment (Perrow, 1999). From this example, crisis communication scholars can diagnose and later identify the interactive complexity within

the system across its subsystems to suggest a crisis management plan grounded in human intervention.

This human intervention is imperative in both the pre-crisis and crisis phase during a normal accident in these high-risk systems. As Perrow (1999) notes, "normal accidents stem from the mysterious interaction of failures, those closest to the system, the operators, have to be able to take independent and sometimes quite creative action" (p. 10). This "operator action", as Perrow puts it, is communicative at its core seeing as multiple operators exist across various subsystems that have the potential of interacting. Thus, the intervention or 'action" produced by the operator in response to the first subsystem's failure during a crisis must be quickly and effectively communicated to other operators across the system. Or, as Perrow (1999) suggests, "the communication must be exact, the dial correct, the switch position obvious, the reading direct, and on-line" (p. 84). Other operators overseeing related subsystems must be made aware of the primary subsystem's malfunction promptly to prevent the failure of their subsystem. To accomplish this, a crisis communication strategy that accounts for the possibility of these accidents occurring must be in place for operators to be aware of how they should intervene and who they should be contacting as the crisis unfolds. Normal Accidents theory provides insight into how these 'mysterious' failures may occur in a complex system, shedding light on the system's high-riskiness based on its interactive complexity. This interconnectivity is known as coupling.

Coupling is the degree of interconnectedness between components within a system (Weick, 1976, 1982; Orton & Weick, 1990; and Perrow, 1984, 1999, 2011). There exists two degrees of coupling – loose and tight. The looseness or tightness of

coupling is the strength of the connection between two subsystems (Perrow, 2011). Weick (1976) was the first to introduce the notion of coupling when he referred to educational organizations as loosely coupled systems. A loosely coupled system is one that contains subsystems that are aware of each other's role but operate primarily in isolation from one another (Burke, 2014; Green & Swanson, 2011; Perrow, 1984; 1999; 2011; and Weick, 1976; 1982). Loosely coupled systems have the advantage that disruptions in one subsystem do not necessarily hinder the overall system's operational goal. Loosely coupled systems allow for various system components to operate freely under their own interests without consequence of impacting another component within the system. As Perrow (1999) notes, "loosely coupled systems tend to have ambiguous or perhaps flexible performance standards, and they may have little consumer monitoring, so the absence of the intended connection can remain unobserved" (p. 91). Thus, the pressure to ensure that all components within a system operate exactly as required is minimal in loosely coupled systems; because the end product's creation is not dependent on the precision in connection between components. However, the downfall of loosely coupled systems is that they are not as efficient and have slower response time due to the weak interconnectivity across the system.

Tight coupling, "is a mechanical term meaning there is no slack or buffer or give between two items" (Perrow, 1999, p.90). Tight coupling is more prominent in extremely high-risk, complex systems that have greater potential for catastrophic consequence in result of a crisis. According to Weick (1976), tightly coupled systems carry four specific criteria: 1) clearly defined rules; 2) organizational members agree on rules; 3) outcomes from rules are clearly defined and a specific procedure is in place to identify when they

are met; and 4) feedback loops are in place to verify the success of the system. He stresses that what differentiates a tightly coupled system from a loosely coupled system is a lack of agreement on a clearly defined process or rule.

Perrow (1999) expands on the four categories considering high-risk, complex systems: 1) time dependent processes; 2) system sequences are invariant; 3) production goal can only be reached one way; and 4) the system has little to no slack. Meaning, the failure of one component results in a direct and quick change within another component. Tight coupling makes for precision in process between subsystems as one relies on the other for the final product to be produced correctly. A tightly coupled system does not allow for various components to behave independently for its own agenda. Instead a tightly coupled system is time-dependent and job-dependent, to where each component must meet its assigned task in its scheduled time to ensure the successful operation of all connected components within the system, and the accurate creation of the final product. For example, a processing plant operates through tight coupling due to it being required to alter its processes for market demands. This change in processes requires operators to proceed quickly so that these changes are noted, reported, and executed with efficiency. By contrast, if a processing plant were loosely coupled these changes in one component would not be met with swift changes in another, and would result in inefficiencies (Perrow, 1984; 1999; 2011).

Tightly coupled systems must be prompt in response to any distresses that may occur to avoid disastrous consequences. However, tightly coupled systems cannot incorporate substitutive aid in response to failure as there is no slack in the system for such input. Instead, these buffers or substitutions are designed-in as part of the system

from its inception. These designed-in aids increase the complexity of the system and cannot always account for interactivity between subsystems that is unexpected. Hence, Normal Accidents theory highlights how some failures that occur within the complex systems are unexpected and can then result in full-blown catastrophes. The complex interactions of a system are those that occur in an "unfamiliar and unexpected sequence that is not visible or immediately comprehensible" (Perrow, 1999, p. 78). This complex interactivity increases because of the tightly coupled and intricate design of the system that is meant to account for all possibilities. Organizations then assume that the more controls, guidelines, and procedures in place decrease the likelihood of an accident. However, Normal Accidents theory suggests the exact opposite. This heightened complexity in design and security increases the likelihood of unexpected interactions that can exist between subsystems. This increase in interactions complicates the system leading to unexpected sequences of failures during an accident that afterwards become a catastrophe, and in turn a crisis. The following section discusses in detail the intricacies related to complex organizations.

Complex Organizations

Much of Normal Accidents Theory highlights almost exclusively complex systems that are technologically advanced and high-risk (e.g. chemical plants, nuclear plants, air craft carriers, etc.). Many scholars have criticized Perrow for his over-emphasis on technology's role within normal accidents; identifying it as 'technological determinism' (see: Le Coze, 2015). Perrow himself highlights in his writing that rooted in his thesis of normal accidents is that technological advancements have become engrained in systems making them highly complex. Though technology is a prominent theme in

normal accidents, it does not erase the role that human behavior and intervention play within complex systems. Vaughan (1996) expands normal accidents theory beyond just technological determinism, and notes that the coexistence of technology and human action can be present within complex systems. He highlights that accidents can occur via the interaction of both technological mishaps and social forces: 'complex and dynamic techno-social coupling' (Coze, 2015, p.277; and Vaughan, 1996). Therefore, normal accidents do not only occur considering the complexity surrounding the system's advanced technology, but can occur due to the complexity of the system's social patterns.

Thus, to qualify as a complex system there is no obligation to being only a technologically high-risk system. Universities, major business corporations, and government agencies serve as complex systems. These systems do not operate in linear interactions, where sequences are familiar and expected, even visible when unplanned. Thus, they are complex in the sense that various sub-systems within the overall system have the potential to reach one another unexpectedly through various means of interaction. Moreover, the looseness and tightness in coupling within such a complex system are not mutually exclusive. As one system can include both loose and tight subsystems within its infrastructure (Green & Swanson, 2011).

These complex systems are not strictly technologically advanced, high-risk systems either, but can be multifaceted organizations; for example: public schools, universities, or multi-departmental companies (Fusarelli, 2002; Perrow, 1991; Weick, 1982). This is key to note, in relation to this study, as SPE is a multi-departmental production company that operates as a complex system. Unexpected interactions within a multifaceted organization can occur between various departments against the system's

overall mission and result in a crisis (Fusarelli, 2002; Green & Swanson, 2011; Lutz, 1982; Perrow 1999; and Weick, 1976; 1982). These various departments serve as the organization's subsystems through the people that operate within them. Similar to a pump in the turbine building of a nuclear plant, particular employees within a specific department constitute that subsystem. For example, the disturbance in the payroll department directly impacts other employee behavior, the goals of the organization, and ultimately its output (Weick, 1982). Leadership must be able to juggle these various demands and goals made of its organization, both the internal (across departments) and external (stakeholders), to maintain cohesion and prevent any organizational failure from happening that could lead to a potential crisis (Spender & Grinyer, 1995).

Perrow (1961) discusses the importance of goals in complex organizations. Perrow distinguishes between "official goals" and "operative goals". He notes that official goals are the general-purpose statements made by organizations to fulfill its legitimacy as an organization. Operative goals are the underlying tactics that are put in place and used to achieve the official goals. For example, if the organization's official goal is to provide exceptional customer service, then its operative goal could be to ensure that 90% of its customer base averages a 4/5 in customer satisfaction on the customer exit survey. Operative goals allow organizations to operationalize how they are going to achieve their official goals through measurable means. Thus, understanding the operative goals of a complex organization allows for the organization to operate in line with fulfilling its intended output. Though official and operative goals have been noted in the literature regarding complex organizations; the interconnectivity of goals between two differing complex organizations has not, nor is it accounted for in Normal Accidents

theory or the literature surrounding complex organizations. Yet, it is worthy of notice to clearly understand the inner workings of complex organizations and their operations, and be able to identify the complexity of SPE as a system.

Summary

Since SPE meets the criteria of a multi-faceted organization, and thus, a complex system, Normal Accidents theory will be used as a theoretical lens to understand the organization's complexity and interconnectivity to shed light on how its 2014 hack crisis transpired and later became a national security crisis.

In sum, a "normal accident" is an inevitable phenomenon in complexly interactive systems. Since it is inevitable, we as communication scholars must identify means to address these accidents as an extension of the organization's normalcy without allowing them to manifest into crises through effective and proactive crisis management tactics. This type of crisis management is possible through increased insight on how the overall system and its sub-systems operate, and how human intervention can be taken in instances of interactive system malfunction. The interactions between subsystems within the system are found to be unexpected sequences that are not seen nor understood upon their happening. The more complex the system, the more likely that a miniscule incident may become catastrophic, due to the strong interdependency of its variables.

Rationale

It is evident through Normal Accidents theory how an unanticipated connection between two independent and unrelated subsystems can occur through nonlinear interactions (Perrow, 2011). In Normal Accidents theory, these two subsystems are related to one major complex system, where a change in one results in a change in the

other, and ultimately affects the system as a whole. This interaction of unexpected sequences is due to the complexity of the system and the coupling between subsystems.

However, research utilizing Normal Accidents theory as the central point of analysis to explain the manifestation of an accident and crisis through the interaction between two independent and unrelated major, complex systems does not exist. Therefore, the following study serves as important research showcasing Normal Accidents theory's versatility in explaining this phenomenon. In the following chapter, I highlight the methodology of this study and how I used case study analysis to fill this gap in research and understand this interaction between two independent complex systems – Sony Pictures Entertainment and the U.S. Federal Government. Also, in the next chapter, I detail how Normal Accidents theory was used as a theoretical lens to analyze the Sony Pictures hack crisis.

CHAPTER III - METHODOLOGY

The current gap in the organizational and crisis communication literature utilizing Normal Accidents theory to understanding the interconnectedness between systems and how one organization's crisis leads to its interaction with a separate organization, and the creation of an additional organizational crisis mandates an in-depth examination of this phenomenon. In this study, I used case study analysis as the primary method to understand how and why the Sony Pictures 2014 hack crisis lead to an interaction with the United States Federal Government, which then created a national security crisis. Throughout the analysis of the case, I used Normal Accidents theory as the guiding lens to examine the case, its events, and the communicative underpinnings that established the interaction between each organization. In this chapter, I first explain what case study analysis is and the type of case study design that was conducted. Second, I justify why case study analysis is the strongest methodology of choice for this study. Third, I provide details on the data collection process. Finally, I discuss how the data was analyzed.

This study posed the following research question:

How did the normal accident within one system (SPE) cause an accident within a separate system (U.S Federal Government) and later transpire into a national security crisis.

Case Study Analysis

Case study analysis is a thorough examination of a phenomenon using various types of evidence to explore and gain an in-depth understanding of that phenomenon. Yin (2013) notes that case study is a form of research that allows researchers to "understand complex social phenomena and gain a holistic and real-world perspective" (p. 674). The

strength and popularity of case study analysis is it provides focus in gaining depth of knowledge pertaining to a specific 'case' by placing boundaries to avoid too broad of study. The 'case' is that which serves as the object of analysis or "phenomenon occurring in a bounded context" (p. 25). Daymon and Holloway (2010) emphasize that case studies are "intensive examination(s), using multiple sources of evidence, of a single entity [case] which is bound by time and place" (p. 105). Other researchers highlight that the case can be bound by time and activity (Stake, 1995), or definition and context (Miles & Huberman, 1994). For the purposes of this research, the case was bound by time and place: Sony Pictures Entertainment (SPE) hack crisis, November 24th, 2014 – January 2nd, 2015.

Based on the typology of case studies introduced by Yin (2003), in this study an "explanatory case study using a single case study design" was employed to analyze the SPE hack crisis. An explanatory case study is "a type of case study used to answer a question to explain the presumed causal links in real-life interventions" (Baxter & Jack, 2008, p. 547). This explanatory case study reveals the communicative casual links between the two organizations to explain how a crisis in one organization caused a separate organization's crisis.

The SPE hack crisis as a case meets Yin's (2013) single case study design rationales – 1) unusual circumstance and 2) testing an existing theory. Thus, the single case study design is used to analyze the SPE hack crisis as an unusual circumstance – a phenomenon that is peculiar, deviates, and contrasts with theoretical norms. Also, it tests an existing theory – Normal Accidents theory – to ensure that the theory is stable in accounting for SPE's organizational accident. Additionally, the single case study design

offers a “deep, narrow exploration” that granted a “detailed, descriptive, and holistic view” of the case (Daymon & Hollaway, 2002, p. 108).

Ultimately, the case study analysis was fitting for this study in that it provided depth of understanding on the SPE hack crisis as an unusual case that tested Normal Accidents theory, while explaining how two separate organizations interacted during the crisis of one. In the next section, I expound on why the case study analysis served as the best method of choice for this study.

Why Case Study Analysis?

Crisis communication research focuses on how entities use various communication strategies to respond to crisis, specifically how communication plays a role in their pre-crisis, crisis, and post-crisis handlings. To accomplish this research goal, crisis communication studies adopt case study analysis as a method of choice to “collect ‘rich’, detailed information across a wide range of dimensions about one particular case or a small number of cases” (Daymon & Holloway, 2002, p.106) pertaining to the crisis in study (see: Coombs & Holladay, 2011; Seeger, 2006; Sellnow & Littlefield, 2005; Ulmer, 2001; Ulmer & Sellnow, 2000).

Case study analysis in the crisis communication arena is used to “increase knowledge about real, contemporary communication events in their context” (Daymon & Holloway, 2010, p. 105). The SPE hack crisis is a real and contemporary communication event that serves as a unique case in connection to risk, crisis, and organizational communication. Thus, a purposeful methodology must be employed to uncover and understand the “many different influences and aspects of communication relationships and experiences” that exist within this crisis (Daymon & Hollaway, 2010, p. 106). Case

study analysis serves this purpose as it is designed to answer the "how" and "why" questions related to a social phenomenon (Yin, 2013). Through its descriptive and interpretive functions, it sheds light on the various complexities that control the communicative aspects that make the case unique (Daymon & Hollaway, 2002; and Sellnow & Littlefield, 2005). Therefore, in this study, to understand how the Sony Pictures hack crisis came to be and why it interacted with the U.S. Federal Government to create a national security crisis, case study analysis was employed to, as noted by Daymon & Holloway (2010), "bring to life the nuances of managed communication by describing a chunk of reality . . . and attempt to offer insights that have wider relevance" (p. 106). These nuances are uncovered, in case study research, by gathering multiple kinds of evidence that are pieced together to describe and explain the case.

More importantly, the case study analysis is a strong methodological choice because it has the advantage of being able to utilize and navigate various types of evidence to establish a thorough examination of the case. As Yin (2003) notes, "the case study is preferred when examining contemporary events, but when the relevant behaviors cannot be manipulated … the case study's unique strength is its ability to deal with a full variety of evidence — documents, artifacts, interviews, and observations" (p. 861). Seeing as the SPE hack crisis is a contemporary event that has already happened, the researcher could not manipulate any behaviors (i.e., experiment) or be on sight (i.e., observational study) to gather data as the case occurred. Therefore, the researcher relied on existing evidence from multiple sources of information and multiple viewpoints to understand the case as a communication crisis event. Baxter and Jack (2008) emphasize the strength behind gathering multiple sources in that "each data source is one piece of

the "puzzle," each piece contributing to the understanding of the whole. This convergence adds strength to the findings as various strands of data braided together promote a greater understanding of the case" (p. 554). In the next section, I discuss how the evidence was gathered and what type of evidence was analyzed in this study

Data Collection

To gain a holistic understanding of the Sony Pictures hack crisis, I used multiple data sources that covered an array of multiple viewpoints to enhance the credibility of the data gathered (Yin, 2013). These multiple data sources were utilized to triangulate the data for a more accurate examination of the crisis event (Efthimiou, 2010).

For the purposes of this study, the data was collected from public communication, various media outlets (e.g., magazines and newspapers), documented interviews, Sony Pictures official statements, and documents authored by the United States Government. Specifically, the sources reviewed included news articles released between November 24th, 2014 – January 2nd, 2015 from different publications and outlets. The articles were compiled from the LexisNexis database by searching the following key terms related to the event: Sony Pictures, Sony Pictures hack, the interview, and North Korea hack on Sony pictures. Internal communication from Sony Pictures Entertainment as well as the United States Federal Government related to the incident – newsletters, bulletins, official statements, presidential orders, company emails, etc. – that were available for public record were also gathered via these various publications. Finally, corroborated interviews of Sony Pictures' employees and government officials were also utilized to analyze the case. Through this collection of multiple sources of evidence, I created an intensive

examination of the Sony Pictures hack crisis, and explanation for how it unfolded and why it interacted with the U.S. Federal Government to form a national security crisis.

Selection of Sources

To piece a definitive compilation of the case, I selected government-direct statements and major American news outlets that covered the SPE hack diligently throughout its occurrence and at its end. A total of nine sources were used to build the case: six major news sources and three government-direct documents. The six news sources included: The New York Times, Time Inc.'s FORTUNE, CNN, NBC News, and Vanity Fair. In addition to being America's elite news sources, these sources included a variety of information to build their coverage. Rather than being a mere summary of the hack's happenings, these news sources included: interviews with SPE leadership and employees, SPE direct emails, government officials' statements, SPE official company statements and bulletins, and FBI commentary for a cohesive and factual representation of the SPE hack. The three government-direct documents included: White House Press Releases, Department of State Press Release, and Department of Homeland Security Press Release. These releases all included commentary from the at-time President of the United States, Barack Obama, at-time United States Secretary of State, John Kerry, and at-time United States Secretary of Homeland Security Jet Johnson. These news outlets and government documents were selected as they all contained direct narrative from SPE officials and government officials who were involved during the crisis. The nine total sources allowed for a holistic understanding of the SPE hack internally, its interactivity with the U.S. Federal Government, and its later evolution to a national security crisis.

Selection of Timeline

A time period of six weeks, from November 24th, 2014 to January 2nd, 2015 was selected for the examination and building of this case. The following is a description of key dates within the timeline. On November 24th, the cyber hackers – Guardians of the Peace (GOP) accessed and hijacked SPE's computer database and server via malware sent through email. Nov. 25th, SPE contacted the FBI and cyber-security firms to assist with containing and fixing the hack and its damages. Dec. 2nd, SPE's CEO Michael Lynton and Co-Chairperson Amy Pascal publicly confirmed the severity of the company-wide hack to the entirety of SPE. Dec 2nd – Dec. 4th, the GOP released multiple "data dumps" where thousands of SPE's private personnel information, emails, and production data were leaked and shared with the public via various internet sites. Dec. 8th, GOP confirmed that the film, *The Interview* was the reason for the hack and demanded that it be removed from theaters. Dec. 8th – Dec. 15th, GOP released more confidential personnel information, emails, and SPE production content. Dec. 16th, the GOP threatened a "9/11 type" terrorist attack against all the theaters that showed *The Interview*. Dec. 16th – 18th, theaters cancel *The Interview* from showing. Dec. 19th, FBI confirmed that North Korea was responsible for the attack. Dec. 19th, at-time government officials, President Barack Obama, Secretary of State John Kerry, and Secretary of Homeland Security Jet Johnson all gave public statements regarding the cyber-attack, SPE's decision, and North Korea's involvement. Dec. 24th, SPE released *The Interview* digitally on select, online video-streaming platforms. Jan. 2nd, at-time president Barack Obama signed an executive order that installed additional sanctions against North Korea in response to the hack and its damages.

November 24th, 2014 is used as the starting point for this study as it marks the day that the GOP made threatening contact with SPE. Although, there are some reports that indicated that a cryptic "warning" was made to SPE much earlier in June 2014 from an unknown source; November 24th also served as the date that the hackers made initial access into SPE's database, and will therefore be used as the starting point for this case. January 2nd, 2015 will serve as the case's end point as it marks the day President Barack Obama released an executive order that imposed additional sanctions against North Korea. Also, by that time *The Interview* had already been released digitally by SPE and seen both nationally and internationally by viewers. In the coming section, I provide an explanation for how the data was analyzed using a descriptive case study method, which includes theoretical proposition's analysis strategy via the explanation building analytic technique.

Data Analysis

Yin (2002) defines a case study as "a contemporary phenomenon within its real-life context, especially when the boundaries between a phenomenon and context are not clear and the researcher has little control over the phenomenon and context" (p. 13). Several approaches to analyzing data within case study research exist. The present study uses a descriptive case study method. This approach stresses "prior development of theoretical propositions to guide data collection and analysis" (Yin, 2002, pp. 13-14). Thus, "Yin emphasizes the necessity that researchers review the relevant literature and include theoretical propositions regarding the case under study before starting to conduct any data collection, which distinguishes it from such methodologies as grounded theory and ethnography" (Yazan, 2015, p. 140). Merriam (1998) explains that case studies can

use purposive sampling to identify the best evidence that highlights the theoretical concepts under scrutiny. Using this approach, case study research is highly descriptive and does not require a more formal content analysis using coding of units of analysis into themes. Rather, the criterion for assessing the validity of the analysis is how closely the "best" evidence represents the concepts as established in the review of literature. If the concepts have been clearly articulated and the supporting materials, often presented from several sources, undoubtedly exemplify those concepts, then the argument for validity should be strong. Data is evaluated in terms of its evidentiary and explanatory value (Yazan, 2015).

Analysis of the evidence to build the case study relies heavily on the conceptualizations of the relevant concepts and draws upon the review of the associated literature. Therefore, the scholarly literature is incorporated throughout the study in a manner that might be uncommon to other methods. The investigator "[draws] systematically from previous knowledge and [cuts] down on misperception" (Stake, 1995, p. 72); concurrently, he or she "gives precedence to intuition and impression rather than guidance of the protocol" (Yazan, 2015, p. 145). It is incumbent on the researcher and reader to "[know] what leads to significant understanding, [recognize] good sources of data, and consciously and unconsciously [test] out the veracity of their eyes and robustness of their interpretations. It requires sensitivity and skepticism" (Stake, 1995, p. 50).

Additionally, Normal Accidents theory's theoretical propositions were used to guide the understanding of the case study (Yin, 2013). Normal Accidents theory's propositions were used to identify conditions for explanations on the case being

examined. This descriptive case study allowed the researcher to link the case to concepts specific to theory; which provided a sense of direction for how the data should be analyzed (Yin, 2013). Additionally, the technique used in conjunction with this descriptive case study is known as - explanation building – analyzing the case by building an explanation for the case itself (Yin, 2013). Specifically, explanation building entails identifying causal links to make sense of why and how the case unfolded in the manner that it did. Also, to avoid any potential problems related to explanation building as an analytic technique, the explanations created reflect the propositions identified in Normal Accidents theory.

Theoretical Propositions

The following are Normal Accidents Theory's theoretical propositions that were used to guide the explanation building technique during the case analysis of this study:

Systems. "Systems are divided into [at least] four levels of increasing aggregation: units, parts, subsystem, and system" (Perrow, 1999, p.70).

Complex Systems. "Systems that contain many interactions that require control, and information about the state of components or processes that is more indirect and inferential" (Perrow, 1999, p.83).

Accidents. "Damage to subsystems or the system as a whole, stopping the intended output or affecting it to the extent that it must be halted promptly" (Perrow, 1999, p.70).

System Accidents. "Unanticipated interaction of multiple failures" (Perrow, 1999, p.70).

Linear Interactions. "Expected and familiar production or maintenance sequence, and those that are quite visible even if unplanned" (Perrow, 1999, p.78).

Complex Interactions. "Unfamiliar sequences or unplanned and unexpected sequences, and either not visible or not immediately comprehensible. (Perrow, 1999, p.78).

Loose Coupled Systems. Systems where the interactivity between subsystems are not dependent upon each other, allow for buffer, and adjustments to be made leniently.

Tightly Coupled Systems. Systems where interactivity between subsystems is very strict and contains no slack. These systems contain all buffers built-in and do not allow for adjustments or leniency during operation.

These theoretical propositions were used to guide the descriptive case study analysis to ensure that a critical and valid explanation of the case was built. Moreover, Normal Accidents theory was expanded to include additional propositions that accounted for the interactivity between two separate, major complex systems during an accident of one. Ultimately, this study's results for the Sony Pictures hack crisis provide an explanation for how the accident unfolded, and why it later became a national security crisis. The following chapter describes in detail the SPE hack crisis case.

CHAPTER IV - CASE ANALYSIS

This chapter reveals the specifics of the SPE hack crisis, how it later transformed into a national security crisis, and describes key proponents that justify the crisis as a normal accident. Specifically, this chapter provides background about the SPE case, explores system failure, subsystem malfunction, and interconnectivity between systems through a timeline narrative of the case study.

Sony Pictures Entertainment Hack: Was it really a crisis?

Crises are not "one-size-fits-all" but vary in type and intensity (Seeger, Sellnow, & Ulmer, 2003). The SPE hack can be identified as an organizational crisis – "a specific unexpected and non-routine organizationally based event or series of events which creates high levels of uncertainty and threat or perceived threat to an organization's high priority goals" (Seeger, Sellnow, & Ulmer, 1998, p. 233) induced by an act of cyber terrorism. In this section, I will explore the SPE hack in three phases to build the case and provide an analysis using Normal Accidents theory to make sense of its happenings; Phase 1 – saying hello: the shakedown of the SPE database, phase 2 – flirting with national security: confidentiality aflame, and phase 3 – it's official: national security crisis over *The Interview*.

Phase 1 – Saying Hello: The Shakedown of the SPE Database

There were no warning signs for SPE before it received its first hack email that contained five links routing to SPE's internal records by the hacker group identifying themselves as the "Guardians of Peace" on the morning of November 24th, 2014 (Elkind, 2015, 66). The email read, "We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world." This

type of attack was foreign to SPE's repertoire of crisis management and served as "a specific unexpected and non-routine organizationally based event" (Seeger et al., 1998, 233). This email was the trigger event, a change in freedom to access resources of importance related to the organizations daily "normal" operations (Stewart, 2000), which lead SPE and its employees directly into the crisis stage. It served as a bifurcation point where the organization's operational normalcy was shaken into an uncertain chaotic situation (Farazmand, 2003). SPE's regular communication platform was at a standstill and at the mercy of this unexpected event. Employees did not have computer, email, or cellphone access, and this resulted in a shift from regular daily operations to operations of crisis response to regain organizational normalcy.

The hackers' initial email allowed for interactivity to ensue with the SPE's computer database. Regular operations using the SPE computer database company-wide include the sending, receiving, and opening of emails; thus, this is considered a normal phenomenon within the system. However, upon opening the initial hack email a complex interaction occurred between the hacker's email and the SPE database. The hacker's email served as one subsystem and SPE's database served as the other subsystem. The two subsystems being unrelated but now connected with each other prompted the accident's formation. Initially this unexpected sequence of interactivity between the email and the database was not visible nor immediately comprehensible (Perrow, 1984). It was not until SPE's entire communication platform was shut down from the hack that an understanding of what was occurring began to become clear for SPE and its leadership. This shutdown marked the beginning of the accident in that various subsystems became damaged leading to a system-wide halt of output for SPE.

During this portion of the crisis stage SPE is interpreting the signal (unexpected trigger event) and attending to its damages. Seeing as this crisis spanned over a long period of time its initial onset did not induce severe emotional arousal as expected in a traditional crisis. Initially, Amy Pascal's (SPE at-time Co-Chairperson) reaction was that it had to be a joke (Seal, 2015). However, being the acting leadership amidst the crisis she persisted to investigate to ensure that her interpretation of the event was a plausible one that led to effective action (Seeger et al., 2003). Through continued communication leaders Pascal and Michael Lynton (SPE at-time CEO) eventually identified the situation's severity, and prompted SPE to take preventive measures to reduce the probability of any data loss. SPE's C.F.O, David Hendler ordered a complete shutdown of the SPE computer database to prevent any further damage until the gravity of the issue was assessed and fully resolved (Seal, 2015).

Phase one of the SPE hack highlights its legitimacy as a crisis as it contains an unexpected event that lead the organization into uncertainty and away from normalcy. This trigger event served as a bifurcation point upon the organization's daily routine. This point shifted the organization's way-of-life. In addition to the complete shutdown of SPE's computer system, employees were instructed to disconnect from Internet access across all their mobile devices and computers. This shut down and disconnect Weick (1988) identifies as a form of enactment known as 'safe inaction' in interest of reaching an accurate diagnosis of the problem until 'dangerous action' can be fulfilled to fully resolve the crisis. Furthermore, this shift in the organization's way-of-life and the disconnect from normalcy highlights a total system accident (Perrow, 1984). A system accident indicates multiple failures in various subsystems across one system. In this case,

various communication subsystems within the SPE system were forced to shut down due to the initial accident that was prompted by the hackers' email. This one component failure lead to multiple other failures throughout SPE that began to interact in unanticipated ways: SPE employees being unable to access internet, communicate via mobile devices, complete work-related tasks via their computers. In result, other business ventures connected to SPE and its employees' duties were thwarted during this timeframe because of the system-wide accident induced by the complex interaction of the GOP email and SPE's subsystem.

Though a system shutdown was fulfilled and SPE did not succumb to negotiating with terrorists at that point (Toros, 2008), phase one was only the initiation of a brewing national security crisis that would extend beyond SPE's organizational borders and into the arms of the United States Federal Government.

Phase Two – Flirting with National Security: Confidentiality Aflame

In a crisis, "organizational members and the public often experience intense emotional arousal, stress, fear, anxiety, and apprehension" (Seeger et al., 2003, p. 9). SPE suffered eight information leaks throughout the hack crisis. Many of these leaks consisted of early movie releases via pirating websites. However, one of the eight leaks released confidential and personal information (i.e., Social security numbers, bank information, credit card information, etc.) of 47,000 Sony employees (Wagstaff, 2014). This type of sensitive information being released for public access via the Internet was detrimental to the organization's members who were directly affected. SPE in turn had to respond accordingly to this massive security breach to ensure the overall safety of its employees; as "an organization's first impulse should be to acknowledge those harmed and do

everything possible to assist them" (Seeger et al., 2003, p. 131). The leadership immediately acknowledged the crisis and provided transparent communication for its employees to manage the issue accordingly. Issue management is "the strategic response to help organizations make adaptations needed to achieve harmony" (Heath, 1997, p. 3). Pascal and Lynton sent a memo to all employees that served as a strategic response for issue management:

> It is now apparent that a large amount of confidential Sony Pictures Entertainment data has been stolen by the cyber attackers, including personnel information and business documents. This is the result of a brazen attack on our company, our employees and our business partners. This theft of Sony materials and the release of employee and other information are malicious criminal acts, and we are working closely with law enforcement . . . While we are not yet sure of the full scope of information that the attackers have or might release, we unfortunately have to ask you to assume that information about you in the possession of the company might be in their possession. While we would hope that common decency might prevent disclosure, we of course cannot assume that . . . We can't overemphasize our appreciation to all of you for your extraordinary hard work, commitment and resolve. (Peterson, 2014, p. 1)

Additionally, the FBI as well as multiple cyber-security firms were sought out to assist in solving the crisis at hand (Seal, 2015). Though Sony was not responsible for the leaks that occurred, since they were acts of terrorism, it was in fact responsible for its employees. It is the role of the organization to take responsibility in reducing the intense emotional and psychological stress that is experienced by its members (Seeger et al.,

2003). Moreover, SPE's employees not only suffered "emotional and psychological" stress but they suffered damages towards their livelihoods, as one SPE employee, who wanted to remain anonymous, stated in an interview with Fortune magazine:

> Things became more clear when it was revealed what information was released. Around Wednesday or Thursday, people started saying: call your bank, change your passwords, set up a new checking account. I was completely irate. Once it got personal, it was just, are you kidding me? Seeing the faces of colleagues with families—they're worried about their life savings, their retirement funds, their kids. (Marikar, 2014, p. 1).

In turn, SPE had to conduct healing, particularly to build a new foundation for its employees' overall security. SPE accepted responsibility for the consequences suffered by its employees and put together positive and progressive measures to overcome and establish stability for its victims (Seeger & Ulmer, 2001).

Interestingly, many large corporations such as SPE have state of the art cyber protection at their disposal that is specifically designed to be the main line of defense for these types of hacks. As Perrow (1984) notes, complex systems have built-in safety designs that are designed with the sole purpose to prevent failure. However, it is these elaborate designs that make the system complex, if not more complex, and more difficult to navigate through during an accident; and that is where SPE failed in its intervention post the initial hack. Once the hack began to release confidential information of SPE employees, the rationale of technological-determinism for the crises' inception falls short. As Vaughan (1996) highlights, in his expansion of Normal Accidents theory from a technological-deterministic theory to a techno-social theory - human intervention plays a

role in the unfolding of accidents, and in Sony's case, crises. Upon receiving the initial scare of a system-wide shut down by the hackers, SPE leadership should have intervened (e.g., social action) accordingly to prevent any further damage from taking place, and lives being negatively impacted. This turning point is similar to Vaughan's (1996) example of the Challenger normal accident: "no fundamental decisions were made at NASA to do evil, rather, a series of rather seemingly decisions were made that incrementally moved the space agency toward a catastrophic outcome' (p. 410). There was no intention from SPE leadership to allow the hackers' continued damage to SPE; yet, its lack of prompt change in behavior in response to the initial hack was the decision that moved SPE to catastrophic outcomes internally (e.g., company and employees), and catalyzed its coupling with the U.S. Federal Government.

The leadership of an organization has extensive power when it comes to decision making especially during times of crisis (Le Coze, 2015). However, as Perrow (1986) highlights, "organizations are tools in the hands of their leaders, but they are imperfect, not completely controlled, tools, and it is a struggle to maintain control over them (p. 134). This is evident when SPE leadership assumed they were making the right decision for the organization considering the initial hack. Its inability to control the happenings within its own organization emphasizes the struggle that it takes to contain an accident when it occurs within a system, if action is not taken quickly and appropriately. This is because organizations are susceptible to their environments and are later shaped by them, while also shaping the environment in return; a true interconnectivity between the organization and external world (Perrow, 1986). Due to the lack of successful intervention by SPE leadership, the entire organization became altered by the accident,

and later the happenings within the organization transferred externally onto society altering the nation's security and creating a separate crisis.

Phase Three – It's Official: National Security Crisis for The Interview

The GOP followed through on each of its cyber threats with precise and destructive action. Initially, this cyber-attack was limited to the boundaries of the SPE organization. However, upon leakage of confidential and personal employee information, the tides turned, and the extent of the aggressor's capabilities became evident and tangible. Thus, SPE was faced with the challenge of responding to the situation accordingly based on the newfound intensity and seriousness of the situation, while still being open to its developing uncertainty. The seriousness of the situation had begun to increase and it became clear to SPE that the initial crisis had spiraled into something beyond its control; and thus, its responses had to become equally as sensitive to the new extremity of the situation (Seeger et al., 2003). Henceforth, SPE's response became communicating the need for assistance from the Federal Government. The Federal Government's subsystem – the FBI – provided its assistance in assessing and containing the hack to the best of its abilities.

This integration of the Federal Government's expertise can be attributed to the phenomenon known as the transformation process. The transformation process, as Perrow (1984) explains, is the redesign of a system through the addition of operator experience to reduce the possibility of interactions that are likely to cause an accident. In this case, the assistance from the Federal Government serves as the addition of operator experience. Its role was to identify how the hackers could access SPE in aim of reducing this interactiveness to avoid further coupling, accidents, and future crises. The Federal

Government brings experience that is rooted in its training against other national security threats, which in turn transformed how the SPE crisis was ultimately handled. The Federal Government's expertise increased the knowledge needed to resolve the problem, seeing as SPE was unable to fix it internally. Additionally, and important to note for this study, this integration of the Federal Government's expertise serves as the initiation point for the between-systems interaction. Because not only is the Federal Government providing its expertise, it is incorporating its relevant subsystems to assist in the containment of the SPE accident. This between-systems interaction is to avoid further impact from the SPE accident onto the Federal Government's organization and its stakeholders – the American people and their livelihood and security.

Amidst all this terror it was still unclear to SPE as to why they were being targeted and why this was happening. Also, during this time SPE continued as planned to release its movie *The Interview* on Christmas day. *The Interview* is a political satire that revolves around the assassination of North Korean Supreme Leader, Kim Jong-Un, which at the time was speculated (later confirmed) to be the catalyst for the cyber-attacks. However, SPE never confirmed a connection between the cyber-attacks and the *The Interview*, nor was it ever made known by the attackers to be the underlying reason for its attacks. It was not until early December when an email from the GOP connected its destruction to reason:

> Stop immediately showing the movie of terrorism which can break the regional peace and cause the War! You, SONY & FBI, cannot find us. We are perfect as much [*sic*]. (Seal, 2015, p. 4)

The GOP reign of terrorism had, through explicit and targeted communication - "FBI cannot find us", bifurcated beyond the walls of SPE and into the hands of the United States Government.

In this moment, a "plausible explanation for the event" (Seeger et al., 2003, p. 127) was established and reasoning for this multi-level crisis was clear. Upon demanding the removal of *The Interview*, the crisis became less targeted on the destabilization of the SPE organization and more of an attack on the United States' guiding principles, particularly the first amendment – American freedom of speech. It sparked the attention and action of major political figures. At-time Secretary of Homeland Security, Jet Johnson stated:

> The cyber-attack against Sony Pictures Entertainment was not just an attack against a company and its employees. It was also an attack on our freedom of expression and way of life. (Johnson, 2014, p. 1)

Furthermore, GOP followed up its demand with ultimatums identifying what would happen if the removal of *The Interview* did not commence:

> We will clearly show it to you at the very time and places. *The Interview* be shown, including the premiere, how bitter fate those who seek fun in terror should be doomed to. Soon all the world will see what an awful movie Sony Pictures Entertainment has made. The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time. If your house is nearby, you'd better leave. Whatever comes in the coming days is called by the greed of Sony Pictures Entertainment. All the world will denounce the SONY. (Cieply & Barnes, 2014, p. 4)

The GOP homed in on the United States' familiarity with crisis intensity (e.g., September 11th) to convey the severity of what may happen if its demands were not met. Though the Federal Government was not at the forefront of communication with the terrorists, this had still become an instance of terrorist negotiation with SPE being at the helm.

Due to these threats to attack any theater that showed *The Interview*, many theaters across the United States cancelled their showings and opted out of showing the movie indefinitely (Cieply & Barnes, 2014). Afterwards SPE cancelled its Christmas day theatrical release of *The Interview* and the movie was shelved until further notice. This decision by SPE solidified in the eyes of the nation that the terrorists had won. It placed the Federal Government in a greater predicament, as it portrayed the United States as willing to succumb to terrorist demands, and forfeit its freedom of speech and expression.

This decision of compliance by SPE then prompted the involvement of the United States President and Secretary of State. This action taken by major political figures that are direct representations of the United States Government highlights the severity of the situation and its inadequate handling. Leadership plays a crucial role during crisis communication. A leader must be "visible, honest, attentive, open, and responsive during a crisis" (Seeger, 2003, p. 241) in terms that respond to the crisis in accordance to the population affected. Once again, SPE's leadership did not react accordingly when they met the demands of the terrorists showing incongruence to essential American values (freedom of speech), and did not lead in terms of the population's needs and values.

Additionally, since the terrorist attack had now become a national security crisis the leadership had changed. Thus, the United States leadership felt required to respond

with immediacy to the people, and be congruent with American values and principles against this act of cyber terrorism. United States Secretary of State John Kerry stated:

> The United States condemns North Korea for the cyber-attack targeting Sony Pictures Entertainment and the unacceptable threats against movie theatres and moviegoers. These actions are a brazen attempt by an isolated regime to suppress free speech and stifle the creative expression of artists beyond the borders of its own country. [. . .] Freedom of expression is at the center of America's values and a founding principle of our Bill of Rights. [. . .] That's why the United States is and always will be a staunch advocate for and protector of the right of artists to express themselves freely and creatively. Whatever one's system of government or views about free expression, there is absolutely no justification whatsoever for an attack like this. [. . .] This provocative and unprecedented attack and subsequent threats only strengthen our resolve to continue to work with partners around the world to strengthen cybersecurity, promote norms of acceptable state behavior, uphold freedom of expression, and ensure that the Internet remains open, interoperable, secure and reliable. (Kerry, 2014, p. 1)

Shortly after, United States President, Barack Obama during his end-of-year press speech made the comment:

> I think Sony made a mistake. We cannot have a society in which some dictators someplace can start imposing censorship here in the United States because if somebody is able to intimidate us out of releasing a satirical movie, imagine what they start doing once they see a documentary that they don't like or news reports

> that they don't like, that's not who we are. That's not what America is about. (Perez, Sciutto, & Diamond, 2014, p. 1)

These statements made by the United States leadership indicate the depth of impact of the crisis, its blossoming from simply being an organizational crisis to a national security crisis, and its severity on the nation.

The Federal Government concluded that the North Korean Government spearheaded the attack. An Executive Order by President Barack Obama was issued in the wake of this cyber-attack that "imposed additional sanctions with respect to North Korea" (The White House, 2015a, p. 1). This document blocked the North Korean Government in dealing with "property or interests in property that are in the United States" (The White House, 2015a, p. 1). Furthermore, President Obama issued legislative proposal that would combat cyber threats and enhance cyber security (The White House, 2015b, p. 1).

The shift from a mere transformation process of assisting one system through the inclusion of another's system's expertise, to a secondary system accident within a separate system (Federal Government) occurred once the reason for the GOP's attack was made evident. Identifying *The Interview* as the motive behind the attacks connected the hackers with North Korea, and its follow-up threats against the U.S. linked its behavior to that of full-fledged terrorism that required national security intervention.

The U.S. Federal Government became the second system to suffer an accident at the hands of the GOP and the poor decision making of SPE leadership. The stripping of *The Interview* from theaters highlighted a direct attack on American values, which is a guiding principle in various subsystems of the Federal Government, such as the

Department of Homeland Security and the Secretary of State's office. SPE's fulfillment with such demands loosely coupled the two systems, as they both failed in upholding guiding American principles – American Freedom and refusal to negotiate with terrorists. This interconnectivity between two major systems, SPE and the U.S. Federal Government, indicates how a crisis can stem from a normal accident due to action taken by leadership that later leads to the halt of its intended outcome (Perrow, 1986). Once this transference in systems occurred, so did its leadership; and thus, the Federal Government took control of the response efforts in attempt to regain normalcy. This type of response effort from the Federal Government is unique in that the Federal Government did not respond to the crisis on behalf of SPE and act as a proxy communicator (Liu, 2011), because SPE did in fact respond to its crisis. What makes this interaction unique is that the Federal Government communicated for itself on its own position and on how SPE handled its system accident and the crisis that stemmed from it, not for SPE. Once the initial accident transformed into a national security crisis, the crisis response became the responsibility of the Federal Government in lieu of its mishandling by the initial failing system. In turn, the Federal Government (the second system) deployed its system resources and communication strategies to handle the crisis. Following, the concluding chapter provides further insight to this complex interaction between systems by noting this research's findings, implications, limitations, and suggests directions for future research.

CHAPTER V - CONCLUSIONS, IMPLICATIONS, AND FUTURE RESEARCH

The purpose of this study was to examine the communicative underpinnings surrounding the SPE hack accident that later transpired into a national security crisis. The study was guided by the theoretical framework of Normal Accidents theory and literature pertaining to complex organizations. Case study analysis was employed as the primary mode of research to analyze the case. The results provided significant conclusions in sociological and risk and crisis communication scholarship.

This chapter presents conclusions specific to the study's research question:

RQ: How does the normal accident within one system (SPE) cause an accident within a separate system (U.S Federal Government) that later transpired into a national security crisis?

The chapter begins with conclusions related to the SPE hack as a justified crisis. I provide results on the SPE crisis to explain how the malfunction of one subsystem interacted with other subsystems to shut down an organization's normal state of operation. Second, I expand the Normal Accidents theory and detail new propositions that help explain how two major systems interacted with one another to form an independent crisis. Proposition 1) common denominator and proposition 2) common goal are introduced, which allow Normal Accidents theory to account for the coupling between two independent systems (SPE & United States Government) through non-linear interactions. Next, the implications of the study are discussed. Then the areas for future research are suggested. Finally, the limitations associated with this study are highlighted.

SPE Hack: A Normal Accident in One System

Perrow (2011) defines an "accident" as a "failure in a subsystem or the system as a whole that damages more than one unit, and in doing so disrupts the ongoing or future output of the system" (66). The trigger event of the crisis shut down multiple units within SPE post-hack. Once the GOP's first email was accessed, multiple units of SPE's computer database were damaged, and afterwards these damages transpired into a complete shut down of the studio's production. The hack itself disrupted SPE's output as a company, due to all employees and ongoing projects being halted to assess the database outage. SPE's future output suffered because *The Interview* was removed from its scheduled release in theaters. Its expected financial gain through the cinematic distribution of *The Interview* across theaters nationwide was disrupted due to theaters closing in reaction to the hack. Thus, the SPE hack is independently a within-system accident as it identified the coupling between the SPE database, its film production, and the film's release in theaters across the United States. The failure of the SPE database (subsystem 1) lead to the shutdown of studio daily operations (subsystem 2), and the removal of the film's release in theaters (subsystem 3).

Moreover, the crisis of SPE amassed victims, another identifier solidifying it as an 'accident'. The release of employees' private personnel information to the public served as 'victim exposure' from damage during the accident (Perrow, 2011). The employees of SPE are operators of the system who have an influence on the organizations' operation, and are so classified as 'first-party victims.' However, SPE employees in this particular case are 'second-party victims', as Perrow (2011) notes these victims are "those associated with the system as suppliers or users, but without influence over it. [. . .] They

are voluntary actors who elect to participate in a system but have no influence over its operation" (p. 68). Because SPE's employees did not directly influence, as operators, the accident's creation to where it is classified as operator-error they cannot be categorized as first-party victims in this case. However, since they voluntarily agreed to a contract of employment with SPE they are obligated to accept any risks that stem from accidents throughout the occupation within the organization.

Lastly, the SPE crisis serves as an organizational system accident that involved unanticipated interaction through loose coupling between various subsystems that resulted in multiple failures. The SPE database serves as one subsystem that was loosely coupled with other subsystems like its employees' performance, theaters' operation across the nation, and *The Interview*'s press circuit. Upon the failing of SPE's database these other loosely coupled subsystems failed, and in turn accounted for a system wide accident. Next, I explain how two independent systems interacted with one another to form a separate crisis.

How Two Independent Systems Suffered an Interconnected Accident

In this case, there existed two main systems that interacted: 1) Sony Pictures Entertainment and 2) U.S. Federal Government. A system is the main governing organization that is responsible for multiple sub-organizations that operate within it that are accountable for playing its role in ensuring the intended output of the entire system is fulfilled. Each system in this analysis contained varying subsystems that were impacted by the crisis (e.g., SPE's computer database and the Department of Homeland Security). Moreover, certain subsystems, such as the FBI, from the U.S. Federal Government were used to assist with crisis response in the SPE system accident. These complex interactions

between these varying systems are loosely coupled since each system's subsystems are not dependent on one other for product output under normal operations. However, to further understand how Normal Accidents theory can account for this case's between-systems complex interaction, this section will introduce and explain two new theoretical propositions: 1) common denominator and 2) common goal, these expand the Normal Accidents theory allowing it to account for and explain the coupling between two independent systems through non-linear interactions.

Common Denominator

A common denominator is identified as a shared feature across multiple people or a shared characteristic across different events. For the purposes of this study, a common denominator is defined as - a guiding principle that is shared and serves dual roles across different and independent major systems. This common denominator can serve as the point of interaction between two independent complex systems, which is sufficient to create a coupled state between the two. In this particular case study, both SPE and the Federal Government's mode of operation is guided by the following common denominators – citizen security and American Freedom of Speech.

The two complex systems may not be aware of their shared common denominator's existence. If a system is aware of the common denominator it should account for its function in its crisis planning, being mindful of potential between-systems interaction. If a system is unaware of the common denominator during normal operations it has no bearing on the system's crisis planning. A system might become aware of the common denominator when an unexpected non-linear change is experienced by one system prompted by a crisis in a different system. Additionally, a threat to a common

denominator shared by various organizations will not always prompt between-systems interactions. For example, many organizations share democratic decision making as a guiding principle, an attack on this principle in one organization may not disrupt other organizations. This means a change in the common denominator under one system may only affect that one system and its various internal subsystems. Thus, the common denominator can produce two possible interactions: 1) within one system or 2) between multiple systems.

A brief example of two local universities in the State of Mississippi interacting with one another in response to a tornado that ravished one of the universities will better explain the role of the common denominator within and between complex systems. Hattiesburg, MS is home to both William Carey University and the University of Southern Mississippi (USM). Under normal circumstances both universities are adversaries in various metrics relating to university standing. Moreover, William Carey and USM are two complex systems that usually operate independently of one another. However, in January 2017 a tornado tore through the William Carey campus leaving it severely damaged and out of commission for normal business operations. In response, USM allocated its facilities to William Carey's students and faculty so that William Carey could maintain its responsibilities throughout the semester. The reason for this intervention by USM to assist William Carey is because of the common denominator that they both share as Mississippi Universities – the academic success and retention of Mississippi based college students. Absent this common denominator that links these two rival universities together there would be no motivating factor for USM to interact with William Carey, an adversary. The tornado served as the threat against the common

denominator and prompted a non-linear interaction between these two independent systems. Without USM's intervention to assist William Carey, the academic success and retention of William Carey students would have suffered greatly. This suffering would have in conjunction negatively impacted the overall academic success and retention of Mississippi college students, which is a guiding principle that is actively upheld by USM. Thus, this common denominator connected these two universities together in response to the crisis of one university. The deterioration of one independent system's ability to uphold the common denominator prompted a separate system to intervene and contain the crisis to prevent the crisis from expanding. In the example above, the inability to sustain the common denominator in one system due to an existing threat is what lead for the interconnectedness between two separate systems. Regarding SPE and the Federal government, it was SPE's failure to uphold the common denominator internally (within system) in response to the cyberattack (organizational crisis) that lead to the coupling between systems, and the manifestation of an even larger crisis at the national level with the U.S. Federal Government intervening.

There were two common denominators that connected the two independent systems, SPE and Federal Government to produce a national security crisis – 1) citizen security and 2) American freedom of speech. The cyberattack on SPE was a direct consequential threat on employee safety; and in response the federal government was motivated to reduce further consequences on American people. Here the principle of citizen security acted as the first common denominator that coupled the two systems (see figure 1).

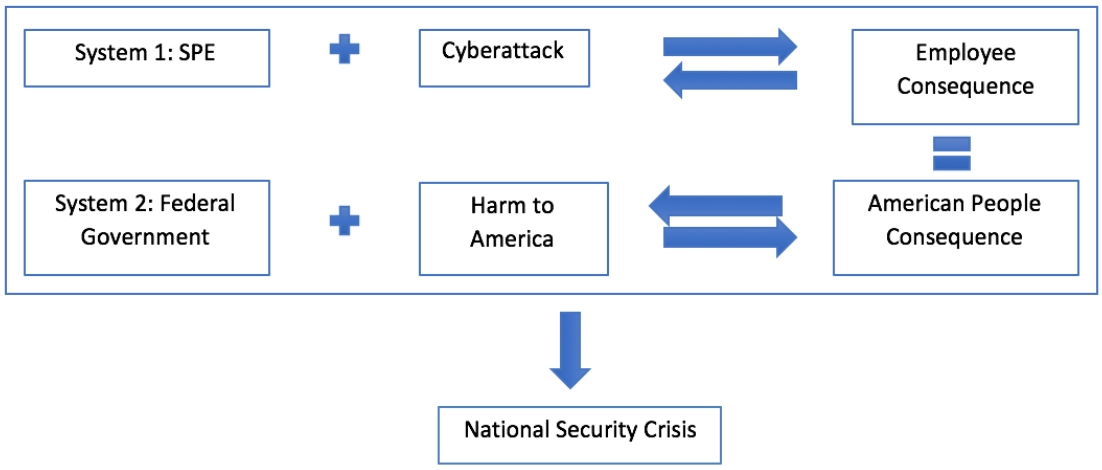

Figure 1. Common Denominator 1 Between SPE and Federal Government

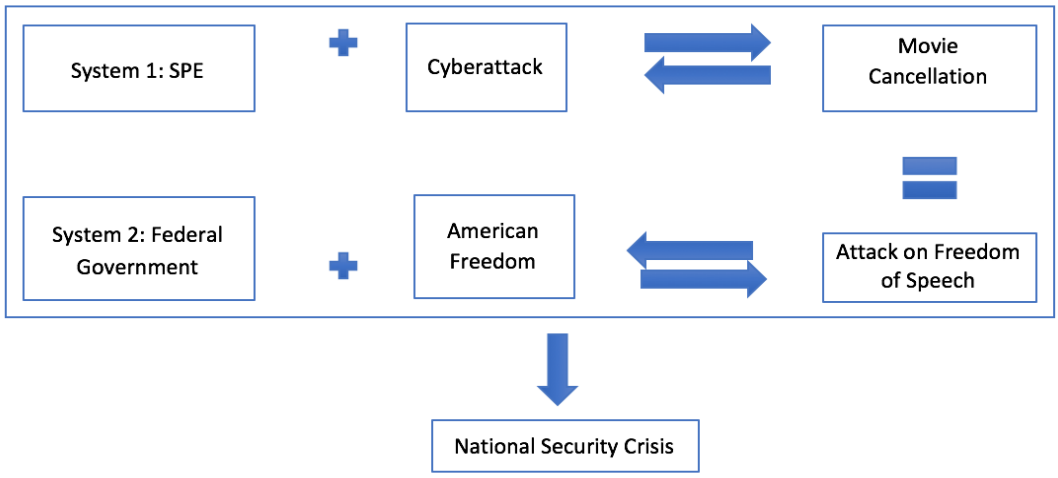

Figure 2. Common Denominator 2 Between SPE and Federal Government

The second being the ultimatum given by the hackers to remove *The Interview* from theaters was an attack on American freedom of speech (see figure 2). These common denominators served as linkage between both SPE and the Federal Government. The cyberattack was a direct threat against these common denominators and SPE's inability to contain the threat accordingly lead the Federal Government to intervene, prompting the resolution of a national security crisis. In addition to the common denominators, this case

highlights that for two separate systems to interact during the crisis of one that another element be met - common goal. Common goal is discussed below.

Common Goal

As noted previously in the review of literature, Perrow (1961) briefly discusses the role that goals play in complex organizations. Perrow goes on to identify "official goals" and "operative goals". Official goals being the general-purpose statements made by organizations to fulfill its legitimacy as an organization. And operative goals being the underlying tactics that are put in place and used to achieve the official goals. However, though official and operative goals are identified in the literature regarding complex organizations; the interconnectivity of goals between two separate complex organizations has not, nor has it been accounted for in Normal Accidents theory. Therefore, in this section, I introduce 'common goal' as a new proposition in extension of Normal Accidents theory to account for the interconnectedness of goals between systems during a crisis.

In layman's understanding, a common goal is a shared agenda for multiple people or a shared mission across various institutions. For this study and the purpose of expanding Normal Accidents theory, a common goal is defined as a general, shared course of action that is sought and tailored by different and independent systems to maintain congruency with their organizational values and principles. A common goal is one of the overarching practices of a system that is utilized to meet the common denominator, dependent on that common denominator's individual responsibility within the system and between systems. For example, if the common denominator is financial longevity, the common goal would be achieving top line revenue growth markers year

after year. Like the common denominator, a complex system can be either aware or unaware of a common goal that exists between them and another system.

In the example of William Carey and USM noted previously, the two systems ostensibly share a common goal – the provision of consistent and high-quality education to Mississippi students. The common denominator that directly guides this goal is student success and retention. If a threat were to ever impact either institution then that would disrupt the common goal of either system, and connect the two systems. The complete destruction of the William Carey campus by the tornado served as that threat and made the university unable to meets its goal of providing a consistent and high-quality education for its students. In turn, USM shared its resources with William Carey to maintain this common goal and uphold the overall common denominator. Any threat to the system becomes a threat to meeting its goal and upholding its guiding principles. When these goals are common and systems have a common denominator, it transpires into a between-systems crisis rather than merely a within-system catastrophe.

SPE and the Federal Government have two common goals that were negatively affected that resulted in a national security crisis: 1) maintenance of system security and 2) autonomously create and share modes of expression. The security breach that released 47,000 SPE employee social security numbers, financial records, and personal information indicated that this terrorist group if they wanted to, through means of cyberterrorism, could hack into the Federal Government and harm other Americans by disseminating their personal information. Therefore, the SPE hack on employee information directly impacts the first common goal. Further, the potentiality of it

occurring beyond SPE walls served as a threat to American security, and merited national security involvement.

The SPE's compliance to the terrorist demand of removing *The Interview* from theaters was a clear violation of the second common goal as it directly prevented SPE from sharing its art. This compliance from SPE misrepresented the United States and portrayed it as a nation willing to succumb to terrorist demands regarding what the U.S. can and cannot produce and transmit, stripping the U.S. of its autonomy to express. United States leadership in turn acted immediately against this threat by making statements in opposition of SPE's compliance towards stripping the movie. The Federal Government's intervention because of SPE's failure to manage the crisis appropriately and maintain the common goal solidified the coupling between the two systems as the SPE organizational crisis transformed into a national security crisis. The hindrance on these common goals perpetuated further nonlinear interactions between SPE and the Federal Government. Also, it showcased how two independent complex systems can be coupled together due to the accident in one that threatens against the common goal.

In sum, the addition of the common denominator and common goal propositions into the proposition repertoire of Normal Accidents theory expands the theory's ability to explain multiple systems interaction. Rather than only accounting for the interconnectivity of subsystems within one complex system, these propositions allow Normal Accidents theory to be used in evaluating how two separate complex systems have the potential of coupling with one another via the identification of their common goals and denominators. Next, this chapter explores the implications that this case study provides the discipline of risk and crisis communication.

Implications

This section identifies the implications of the SPE hack case study. First, implications related to the expansion of Normal Accidents theory are discussed. Second, the common denominator and common goal and their role in Normal Accidents theory is addressed. Finally, the use of these concepts by crisis communication practitioners is determined. To start, the implications of Normal Accidents theory are noted.

Expansion of Normal Accidents Theory

Perrow (1984) introduced Normal Accidents theory as a theory to explain why complex systems contain accidents. He noted that systems contain subsystems that are either loosely or tightly coupled, which allows them to interact with one another and that a disruption in one subsystem may lead to the failure of the entire system due to its interconnectivity with other subsystems. However, Perrow only discussed the accidents that stem within a single system and did not mention the possibility of a between systems accident. This case study expanded Normal Accidents theory so that it could explain how two independent systems can interact with one another in response to one system's accident. It showcases that organizations share commonalities that once disrupted in one organization could potentially impact another. Crisis communication scholars should be more cognizant of these commonalities to better plan for the potentiality of a crisis occurring between systems. These commonalities are the common denominator and common goal, the following section discusses their role within Normal Accidents Theory.

Common Denominator and Common Goal

The common denominator and common goal provide an accentuation for how two independent systems can find themselves interconnected in light of a crisis impacting one of them. The common denominator indicates the shared common principles that each system carries. The common goal is the shared course of action carried out to uphold a certain common denominator. This case depicts how both SPE and the U.S. Federal Government share common denominators and goals that once thwarted at the helm of the cyber-attack lead to their coupling as systems and a national security crisis. The identification of the common denominator and common goal provides crisis communication practitioners with a vantage point for communication strategy development between two separate organizations. Furthermore, these propositions provide a linkage that explains how a private organization like SPE can interact with a public entity such as the U.S. Federal Government in response to a crisis. Strategies that would help organizations better communicate with one another to accommodate the potentiality of a crisis impacting them simultaneously. The utilization of these concepts in crisis assessment, crisis response development, and crisis planning will deem beneficial in the pre, during, and post stages of a crisis. The application of these propositions is addressed in the following section.

Application of New Propositions

Practitioners should utilize these propositions to initially identify the probability of an interaction between two independent organizations during the crisis of one. The uncovering of interconnectedness between organizations could lead to extensive crisis prevention plans that take into consideration the motivation that exists and prompts

interaction with another organization in aim of resolving the crisis. For example, Hollywood production companies are now more alert in their crisis planning to the assistance of the Federal Government in relation to cyber security threats that compromise their organization's safety and product output. Furthermore, awareness of common denominators and common goals will allow practitioners to assess past crises with more diligence to better uncover the underlying reasons for interconnectedness between systems. Also, with the common denominator and common goal in mind, practitioners can be more thoughtful in their crisis response development so that they uphold the systems' common denominator(s) and continue to meet the systems' common goal(s) without the risk of magnifying the already existing crisis. For example, if crisis communication practitioners at the time of the SPE hack crisis were vigilant to the common goal – autonomously sharing modes of expression – then they could have responded differently, by not complying to the terrorist demands, and in turn would have prevented the organizational crisis developing into one of national security.

This section highlighted the implications that stem from the SPE hack case. Implications related to the expansion of the Normal Accidents theory and what it means to the field of crisis communication was noted. The implications revolving the addition of the common denominator and common goal as theoretical propositions were discussed. Finally, implications on the application of these new propositions by crisis communication practitioners was addressed. In the following section, areas of future research are explored.

Future Research

This case study has provided significant additions and expansions to Normal Accidents theory that enhance the scholarship and practice of crisis communication. This section notes the academic and practical directions that can be made through the findings of this research. First, research exploring existing cases that contain the theoretical propositions provided in this study is proposed. Secondly, research related to cases that may contain only one of the propositions, or an evolution of either of the propositions, and how that affects a crisis is addressed. Finally, research focused on enhancing the understanding of accidents that occur between systems using the modified Normal Accidents theory is suggested. Research areas in existing cases are noted first.

Existing Cases

This case study highlights how the coupling of two independent complex systems is possible and can be determined using the modified Normal Accidents theory. Currently, there exist cases that have shown signs of the theoretical propositions proposed in this study, and they should be assessed using this modified Normal Accidents theory to better understand the interconnectedness taking place between separate systems during a crisis. One case being the William Carey University tornado crisis and its coupling with the University of Southern Mississippi. An assessment of this case could enlighten other academic institutions nation/worldwide on how to interact with neighboring institutions for help in response to a natural disaster crisis impacting their campus. Another case is the FBI vs. Apple Inc. encryption dispute. Its unfolding could be studied using the new Normal Accidents theory propositions to make sense of how the FBI and Apple became interconnected systems in response to the 2015 San Bernardino

attack. Both organizations shared the common denominator – American security and privacy; however, they were at opposing ends on how they handled the crisis and the roles they each played as independent organizations while interacting. These cases, if studied using the new propositions suggested in this study would provide novel insight to the crisis communication discipline in further understanding between-system interaction. The following section addresses how future research should examine obscure cases that do not contain both propositions simultaneously, but each proposition individually and how that impacts the crisis and systems.

Obscure Cases

The SPE hack crisis uncovers the existence of both the common denominator and common goal operating simultaneously amidst a crisis. However, not all between-systems crises will contain both propositions, some may contain one or the other, or different evolutions of these propositions. For example, future studies could explore the possibility of uncommon denominators and uncommon goals. In other cases, it is likely that the same denominators and goals that are common between two separate organizations may also contradict one another dependent on the specific crisis and based on how each organization chooses to respond.

Ultimately, it is vital for the crisis communication discipline to study cases that contain these evolutions as well as only one proposition during a crisis and assess how these variations change the progression of the crisis, the relationship between the two affected systems, and any other subsequent analyses. This type of research will indicate which of the propositions carries more weight in impacting the interconnectedness between systems in a crisis, and whether the propositions' opposing evolutions have any

impact on the case and its end result. Uncovering such insight will allow crisis communication practitioners to develop crisis plans that are geared towards addressing each specific proposition to better handle the intricacies of the accident.

Between-System Accident Dynamic

Currently, there is not much existing research that studies uses Normal Accidents theory to study the interaction between two independent complex systems during a crisis, especially systems of varying nature – private vs. public. Existing research using Normal Accidents theory primarily focuses on strictly one system, its subsystems, how the system is affected by a crisis, and a crisis communication strategy for within-system response. However, from this case study it is evident that more cases involving between-systems interaction in face of a crisis should be looked at using Normal Accidents theory; in order to identify fresh perspective on future crisis communication and strategies. If more research revolving between-systems interaction is conducted it will provide the crisis communication discipline with further scholarship that supports a means to accommodate these unique crises. Furthermore, with more between-systems focused research new expansions to theories such as Normal Accidents theory will occur allowing us to better study future cases with more versatile theories. It is essential to conduct this type of research so that organizations become aware of their interconnectivity with other organizations. And crisis communication practitioners can then teach organizations' stakeholders how to navigate within this potential interconnectedness during times of accidents and crisis. Next, I address the limitations of this research.

Limitations

The following section will consist of a forthright discussion of the limitation of this research. Specifically, I address the information outlets utilized to compile the data, and the types of sources used as data for this case. Initially, I explore the information outlets used in this project.

Information Outlets

For this study, only American news outlets and government documents were used and examined for the case. International news outlets, and the North Korean Government's communication may have provided a different perspective on the case and the crisis's unfolding. However, seeing as the U.S. was the victim in this crisis, it made sense to narrow the frame of reference to that of the American media for consistency in coverage and government communication. Following, I address the types of sources used to build this case and how it is a potential second limitation.

Data Source Type

Only existing sources were used to build the case. Should the study have included interviews of SPE employees (i.e., victims of the hack) conducted by the researcher, the shaping of the case may have been different. Nonetheless, the media outlets acquired for this study contain interviews with both SPE employees, leadership, and government officials; which all support the building of the case's timeline and happening from those directly impacted and involved. Ultimately, future studies involving the SPE hack of 2014 could include information from international news outlets and international government documents to broaden the perspective of the case. Furthermore, direct interviews by the researcher with SPE employees, leadership, and government officials

who were either involved or impacted during the hack would potentially provide a deeper understanding of the crisis and how it unfolded.

Overall Conclusion

Accidents occur in organizations and are deemed normal, especially when these organizations are complex ones. The Sony Pictures Entertainment hack crisis of 2014 spiraled into a national security crisis that required the intervention of the United States Federal Government. This crisis was a unique organizational crisis as it connected a private organization and public entity, who normally would not interact with each other, in response to one system accident. Normal Accidents theory accounts for within-systems accidents arising from subsystem interconnectedness and malfunction. However, it does not explore the interconnectedness of two separate systems in response to a crisis in one. This case study expanded Normal Accidents theory and used it to explain the interconnectivity between two separate, major complex systems.

Consequently, this crisis proved a worthy case study for crisis communication scholars and practitioners. It displayed a novel phenomenon that limited crisis communication research has explored: between private and public organization interaction during a high stress crisis event analyzed using Normal Accidents theory. This research, using the SPE hack crisis as its primary case, expanded normal accidents theory by introducing two new propositions: 1) common denominator and 2) common goal, that accounted for between-systems interaction during a crisis. Moreover, the study answered its research question: the reason for why an accident in one system can lead to an interaction within a different system and later catalyze a separate crisis is because of the harm to the systems' common denominators and common goals. This study demonstrated

the importance of the common denominator and common goal in identifying the potential coupling of two systems in light of a crisis. This research provided progressive impact to the risk and crisis communication discipline through its expansion of the Normal Accidents theory and practical findings. The SPE hack crisis which later became a national security crisis is a strong case study for assisting in the development of future crisis responses, crisis planning, and crisis assessment.

REFERENCES

Atalay, A., & Sanci, G. (2015). Cyberterrorism and Turkey's Counter Cyberterrorism Efforts. *Information & Security*, *32*(1), 1-23. doi:10.11610/isij.3203

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, *13*(4), 544-559.

Benoit, W. L. (1995). Sears' repair of its auto service image: Image restoration discourse in the corporate sector. *Communication Studies*, *46*(1-2), 89-105.

Burke, W. W. (2014). Changing loosely coupled systems. *The Journal of Applied Behavioral Science*, *50*(4), 423-444.

Cieply, M., & Barnes, B. (2014). Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm. *The New York Times*. http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html?_r=0

Coombs, W. T. (1999). Information and compassion in crisis responses: A test of their effects. *Journal of public relations research*, *11*(2), 125-142.

Coombs, W. T. (2009). Conceptualizing crisis communication. In R. L. Heath & H. D. O'Hair (Eds.), *Handbook of crisis and risk communication* (pp. 100-119). New York: Routledge

Coombs, W. T. (2010). Parameters for crisis communication. *The handbook of crisis communication*, 17-53.

Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding*. Sage Publications.

Coombs, W. T., & Holladay, S. J. (1996). Communication and attributions in a crisis: An experimental study in crisis communication. *Journal of public relations research*, *8*(4), 279-295.

Coombs, W. T., & Holladay, S. J. (Eds.). (2011). *The handbook of crisis communication* (Vol. 22). John Wiley & Sons.

Daymon, C., & Holloway, I. (2010). *Qualitative research methods in public relations and marketing communications*. Routledge.

Efthimiou, G. G. (2010). Regaining Altitude: A case analysis of the JetBlue Airways Valentine's Day 2007 crisis. *The handbook of crisis comm*.

Elkind, P. (2015). Inside the Hack of the Century. (cover story). *Fortune*, *172*(1), 64-89.

Farazmand, A. (2003). Chaos and transformation theories: A theoretical analysis with implications for organization theory and public management. *Public Organization Review*, *3*(4), 339-372.

Fusarelli, L. D. (2002). Tightly coupled policy in loosely coupled systems: Institutional capacity and organizational change. *Journal of Educational Administration*, *40*(6), 561-575.

Gotham, K. F. (2012). Cascading crises: the crisis-policy nexus and the restructuring of the US housing finance system. *Critical Sociology*, *38*(1), 107-122.

Green, J., & Swanson, T. (2011). Tightening the system: reference as a loosely coupled system. *Journal of Library Administration*, *51*(4), 375-388.

Heath, R. L. (1997). *Strategic issues management: Organizations and public policy challenges*. Sage Publications.

Heath, R. L., & O'Hair, H. D. (Eds.). (2010). *Handbook of risk and crisis communication*. Routledge.

Herrmann, R. K. (1984). Foreign policy decision-making: Perceptions, cognition and artificial intelligence. In D. A. Sylvan & S. Chan (Eds.), Foreign policy decision-making. New York: Praeger.

Janczewski, L. (Ed.). (2007). *Cyber warfare and cyber terrorism*. IGI Global.

Johnson. J., Department of Homeland Security. (2014). *Statement By Secretary Johnson On Cyber Attack On Sony Pictures Entertainment* [Press release]. https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment

Kennedy, S. D. (2001). Security technology and other issues. Information Today, 18(11), 34–35

Kerry. J., U.S. Department of State. (2014). *Condemning Cyber-Attack by North Korea* [Press release]. http://www.state.gov/secretary/remarks/2014/12/235444.htm

Lee, Y., Kwon, H., Lee, J., & Shin, D. (2015). Development of Countermeasures against North Korean Cyberterrorism through Research Case Studies.*Korean Journal Of Defense Analysis*, *27*(1), 71-86.

Le Coze, J. C. (2015). 1984–2014. Normal Accidents. Was Charles Perrow Right for the Wrong Reasons?. *Journal of Contingencies and Crisis Management*, *23*(4), 275-286.

Liu, B. F., Horsley, J. S., & Levenshus, A. B. (2010). Government and corporate communication practices: do the differences matter?. *Journal of Applied Communication Research*, *38*(2), 189-213.

Lutz, F. W. (1982) Tightening up loose coupling in organizations of higher education. Administrative Science Quarterly, 27, 653-669.

Marikar, S. (2014) "I Work at Sony Pictures. This Is What It Was Like After We Got Hacked." Fortune, December 20. Retrieved from http://fortune.com/2014/12/20/sonypictures-entertainment-essay/

Matusitz, J. (2014). The Role of Intercultural Communication in Cyberterrorism. *Journal Of Human Behavior In The Social Environment*, *24*(7), 775-790. doi:10.1080/10911359.2013.876375

Merriam, S. B. (1998). *Qualitative research and case study applications in education*. San Francisco, CA: Jossey-Bass.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Miller, D., & Slater, D. (2001). The Internet: an ethnographic approach.

Millner, A. G. (2011). *Strategic ambiguity and proxy communication in organizational crises: The Peanut Corporation of America case*. University of Kentucky.

Millner, A. G., Veil, S. R., & Sellnow, T. L. (2011). Proxy communication in crisis response. *Public Relations Review*, *37*(1), 74-76.

Orton, J. D., & Weick, K. E. (1990). Loosely coupled systems: A reconceptualization. *Academy of management review*, *15*(2), 203-223.

Paul, D., Bugnar, N. G., & Mester, L. E. (2015). Terrorism and its impacts on the tourism industry. *Romanian Review on Political Geography/Revista Româna Geografie Politica*, *17*(1).

Perez, E., Sciutto, J., & Diamond, J. (2014). Obama: Sony 'made a mistake'. *CNN*. http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/.

Perrow, C. (1961). The analysis of goals in complex organizations. *American sociological review*, 854-866.

Perrow, C. (1967). A framework for the comparative analysis of organizations. *American sociological review*, 194-208.

Perrow, C. (1984). Normal accidents: Living with high risk systems.

Perrow, C. (1999). Organizing to reduce the vulnerabilities of complexity. *Journal of contingencies and crisis management*, *7*(3), 150-155.

Perrow, C. (2011). *Normal accidents: Living with high risk technologies*. Princeton University Press.

Peterson, A. (2014). The cyberattack on Sony Pictures made employees collateral damage. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/12/03/the-cyberattack-on-sony-pictures-made-employees-collateral-damage/?utm_term=.6ba5a6eda34c

Seal, M. (2015). An Exclusive Look at Sony's Hacking Saga. *Vanity Fair*. Retrieved from http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg

Seeger, M. W. (2002). Chaos and crisis: Propositions for a general theory of crisis communication. *Public Relations Review, 28*(4), 329-337.

Seeger, M. W. (2006). Best practices in crisis communication: An expert panel process. *Journal of Applied Communication Research*, *34*(3), 232-244.

Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (1998). Communication, Organization, and Crisis. *Communication Yearbook 21*, 231. Thousand Oaks, CA: Sage.

Seeger, M. W., & Ulmer, R. R. (2001). Virtuous responses to organizational crisis: Aaron Feuerstein and Milt Colt. *Journal of Business Ethics*, *31*(4), 369-376.

Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (2003). *Communication and organizational crisis*. Greenwood Publishing Group.

Sellnow, T. L., & Littlefield, R. S. (Eds.). (2005). *Lessons learned about protecting America's food supply*. Institute for Regional Studies, North Dakota State University.

Spender, J. C., & Grinyer, P. H. (1995). Organizational renewal: Top management's role in a loosely coupled system. *Human Relations*, *48*(8), 909-926.

Stake, R. E. (1995). The art of case study research. Thousand Oaks, CA: Sage.

Stewart, F. (2000). Crisis prevention: Tackling horizontal inequalities. *Oxford Development Studies*, *28*(3), 245-262.

The White House. (2015a). *Imposing Additional Sanctions with Respect to North Korea* [Press release].

The White House. (2015b). *Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts* [Press release]. Retrieved from https://www.whitehouse.gov/the-press-

office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

Toros, H. (2008). We don't negotiate with terrorists!': Legitimacy and complexity in terrorist conflicts. *Security Dialogue*, *39*(4), 407-426.

Ulmer, R. R. (2001). Effective crisis management through established stakeholder relationships: Malden Mills as a case study. *Management Communication Quarterly, 14*(4), 590-615.

Ulmer, R. R., & Sellnow, T. L. (2000). Consistent questions of ambiguity in organizational crisis communication: Jack in the Box as a case study. *Journal of Business Ethics*, *25*(2), 143-155.

Vaughan D. 1996. The Challenger Launch Decision: Risky Technology, Culture and Deviance at NASA. University of Chicago Press: Chicago

Venette, S. J., Sellnow, T. L., & Lang, P. A. (2003). Metanarration's role in restructuring perceptions of crisis: NHTSA's failure in the Ford-Firestone crisis. *Journal of Business Communication*, *40*(3), 219-236.

Wagstaff, K. (2014). Sony Hack Exposed 47,000 Social Security Numbers, Security Firm Says. Retrieved December, 2016, from http://www.nbcnews.com/storyline/sony-hack/sony-hack-exposed-47-000-social-security-numbers-security-firm-n262711

Weick, K. E. (1976). Educational organizations as loosely coupled systems. *Administrative science quarterly*, 1-19.

Weick, K. E. (1982). Management of organizational change among loosely coupled elements. *Change in organizations*, *375*, 408.

Weick, K. E. (1988). Enacted sensemaking in crisis situations [1]. *Journal of management studies*, *25*(4), 305-317.

Weimann, G. (2005). Cyberterrorism: the sum of all fears?. *Studies in Conflict & Terrorism*, *28*(2), 129-149.

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134-152. Retrieved from http://www.nova.edu/ssss/QR/QR20/2/yazan1.pdf

Yong-joon, L., Hyuk-jin, K., Jaeil, L., & Dong-kyoo, S. (2015). Development of Countermeasures against North Korean Cyberterrorism through Research Case Studies. *Korean Journal of Defense Analysis*, *27*(1), 71-86.

Yin, R. K. (2002). Applications of Case Study Research Second Edition (Applied Social Research Methods Series, Volume 34).

Yin, R. K. (2013). *Case study research: Design and methods*. Sage publications.