Thinking Like a Futurist:

Investigating the Theories and Processes of Threatcasting Post-Analysis

by

Jason Brown

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

Approved April 2021 by the
Graduate Supervisory Committee:

Andrew Maynard, Chair
Jason Robert
Brian David Johnson

ARIZONA STATE UNIVERSITY

May 2021

ABSTRACT

Threatcasting is a foresight methodology that examines the worst of potential future changes by imagining and crafting a fictional (but very plausible) story of a person, in a detailed setting, experiencing a threat. In this dissertation, I investigate the processes and techniques of threatcasting, focused primarily on the post-analysis phase, and demonstrate it as an open methodology that can embrace varied ways to analyze raw data and seek conclusions. I incorporate best practices of narrative and thematic analysis, qualitative analysis, grounded theory, and hypothesis-driven theories of inquiry. I use interviews from futurists trained on threatcasting ways of thinking and compare two case studies - one using a grounded theory approach on the future of weapons of mass destruction and cyberspace and the other using a hypothesis-driven approach on the future of extremism - to investigate the efficacy of different theoretical approaches to analysis. I introduce definitions of novelty and ways to assess how a novel finding may have more impact on the future than it appears at first glance. Often, this impact comes more from what is not present in threat scenarios than what is included. Finally, I illustrate how threatcasting, as a practice, is a valuable contribution to those in a position to be responsible architects of a better future.

DEDICATION

To Ariel, Ellie, Noah, and Lydia. You bless me each day.

ACKNOWLEDGMENTS

I am eternally grateful to my supervisory committee for pushing me through to the finish line: to Andrew for allowing me to run wild in our discussions on the future of artificial intelligence and human existence, Films from the Future, and the Pudding Club; to Jason for keeping the questions coming, aligning me to the straight-and-narrow of ethical futures thinking, and for convincing me that my writing isn't awful; and to Brian for the much-needed mental checkups, stories about the blustery Pacific Northwest, and for the friendship and mentorship that I will treasure forever. I am also indebted to my colleagues at the Threatcasting Lab for giving so much of their time to help my projects succeed: Cyndi Coon, Renny Gleeson, Josh Massad, Ali Draudt, and Natalie Vanatta. I would also like to acknowledge the U.S. Army Advanced Civil Schooling program and the sponsorship of the Army Cyber Institute at West Point for sending me to school again in pursuit of this degree. Finally, I am genuinely grateful to my family at home for their patience, tolerance, and forgiveness – it is to them that I dedicate this work.

TABLE OF CONTENTS

CHAPTER Page

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Future Shock and Prediction

Fifty years ago, two journalists -- a husband and wife team -- tried to make sense of the intense social, political, and technological pace of life they saw all around them. By analyzing the "twin forces of acceleration and transience" (Toffler, 1970, p. 19), Alvin and Heidi Toffler captured and described one of the most uncomfortable yet powerful effects humanity has experienced in its purported 800 lifetimes of existence: *unavoidable change*.

As they brought the drivers of this change to light, the Tofflers posited that the next lifetime, the 801st since the advent of humankind, according to them, would need to come to grips with change in ways never before experienced and in ways we have yet to imagine. In essence, how we prepare today sets us up for the inevitable shock that comes with tomorrow's arrival. The Tofflers describes "future shock" as the

> "shattering stress and disorientation that we induce in individuals by subjecting them to too much change in too short a time. [It is] the dizzying disorientation brought on by the premature arrival of the future. It may well be the most important disease of tomorrow" (1970, p. 4, 13).

Future shock, as I think the Tofflers intended, is an overwhelming sense that tomorrow will be so different that it is difficult to be adequately prepared and leaves us paralyzed to make decisions today that may end up being obsolete in just a short time - so why bother making them?

Despite the popularity and compelling perspective of the Tofflers' mildly pessimistic argument, I do not entirely agree. It is prudent to assume that change is coming our way and that it is rather difficult to pinpoint that change precisely, but the lack of clarity doesn't have to be paralyzing. That is, we can imagine, visualize, and understand how these future changes should show up, and we can do something about them. In essence, studying the future with purpose and with repeatable processes can whittle the vastness of anything-is-possible down to a manageable set of plausible futures that we can spend more of our energy focusing on (Hines & Bishop, 2013). More importantly, process-driven studies of the future are more likely to identify the conditions and events that precede impending change.

Occasionally, these processes will stumble upon or gradually piece together certain unexpected events that are novel, unique, or maybe even unprecedented. One of the goals of this dissertation is to rigorously investigate the analytics, imagination, and responsibility required to think like a futurist and create a repeatable process for thinking about any type of future.

Assessments of the future can be in pursuit of achieving utopia, they can be in pursuit of avoiding dystopia, or lie somewhere in between. In any case, mundane and drab assessments are quickly relegated to the trash bin. A good futurist meticulously assesses political, economic, social, technological, and other trends, understands complex systems, and recognizes how organizations need to navigate the windy road between now and the future in order to achieve their goals. A *great* futurist, on the other hand, recognizes that the future is about people, and the job of a futurist is to "*get it right*"

rather than to "*be right"* (Johnson, 2021, p. 33, italics in original). So how do we get it right?

I am confident that no one has cornered the market on predicting the future. As a futurist, I also generally oppose practices that claim to predict the future. Prediction is the pedestal on which someone stands when they want to flash their ego rather than work towards understanding how people fit into the future. Of course, this statement is narrowly aimed at those practices that produce statements like "this will happen on such-and-such date with that percentage of confidence."

In no way does my opposition to prediction attempt to lessen the necessity and value of fields such as predictive analytics (DiFranza, 2021) or predictive data science (Oden Institute for Computational Engineering & Sciences, 2021). These fields use data science, high-performance computing, artificial intelligence, and mathematical modeling to provide accurate assessments of "high-consequence applications in science, engineering and medicine" (Oden Institute, 2021). These assessments have real-world consequences, such as advising city leadership whether a hurricane's path necessitates a wide-scale evacuation. But until computers can grasp the complex connections between "time, space and causality" (Marcus & Davis, 2019) - something humans intuitively do - the best predictions are still going to be assessments and forecasts made with a solid dose of human intuition and bias.

On the other hand, I offer a way to avoid, or at least lessen, the shock of future change. This is by exercising solid data and situation analysis techniques, incorporating thoughtful imagination, and practicing responsible future design that readily identifies novel ideas and prepares decision-makers to enact change now. To do this, I want to

answer a few simple questions. First, what is this thing called threatcasting, and assuming it works as advertised, how does it help futurists "get it right" about future events we want to avoid? Second, how does someone go about learning how to use threatcasting in the right way? Third, what does threatcasting teach all of us about how to think like a futurist and make decisions today that will positively impact those who come after us?

In this project, I explore how threatcasting, a robust foresight methodology, can be further understood and operationalized to provide an adaptable method for addressing and navigating through future shock. In general, by studying and operationalizing threatcasting, I seek to understand the kinds of questions we can ask about the future that are elusive to many other methods. Other methods often seek the path to achieving utopia, or at least chase after a "better" future - however ambiguously "better" is defined - while threatcasting uniquely aims to understand the futures we most certainly want to avoid. How does answering these questions prepare us for resisting future shock in ways that other investigations of the future do not? More importantly, when does an assessment of a future threat rise above the mundane and become something that fundamentally changes how we see the world? Those rare discoveries teach us something about ourselves and about how we previously saw the world radically needs to change. I call this idea *finding evolutionary novelty*.

I will discuss the idea of finding evolutionary novelty in Chapter 6, but I want to introduce the concept quite early, as it will take several chapters to set the foundation for my hypothesis. I consider discovering an evolutionary novelty the ultimate aim of a futurist, and the analytical methods used in threatcasting are uniquely situated to fulfill this aim. I am reasonably sure there is no magic formula - no silver bullet - that is best

suited for discovering evolutionary novelty, as it certainly depends on the context and goals of one's threatcasting project. Still, I submit there are three attributes that futurists should strive to adopt that will make them more sensitive and aware of how to elicit that hyper-novel finding from one's data. Simply said, to think like a futurist, one must have *analytics*, *imagination*, and *responsibility*. I will elaborate on these attributes momentarily.

In the sport of orienteering, participants navigate across miles of forest, hills, rivers, and other types of terrain to seek out flags hidden at various locations. Those who find their points in a specific order in the shortest time win the race. To be successful, participants need three things: a map of the area, a magnetic compass, and a set of field craft skills (a global positioning device is often considered cheating to true orienteering enthusiasts). These fieldcraft skills include understanding how to interpret the symbols on the map, how to calibrate one's pace count to measure how far one has traveled, how to relate the map to the terrain, and a sense of when to deviate from the shortest theoretical route to avoid being delayed by upcoming obstacles or untraversable terrain. In orienteering parlance, the threatcasting process is the compass that guides the journey to finding evolutionary novelty. In contrast, the set of assessments and findings we as futurists present to others is the map, while the triad of analytics, imagination, and responsibility is the fieldcraft needed to understand how to match the map and the compass to the terrain.

Introduction to Foresight

Imagining what the future holds has been a pastime of humanity since time immemorial, yet only recently have scientists and researchers developed it into a field of study. Ideas like prediction, forecasting, foresight, futures studies, imagination, planning, and so on describe the drive to understand and prepare for events and circumstances headed down the pathway of time. In this dissertation, I prefer to use the concept of *foresight* to describe the academic and purposeful study of the possibilities of the future. The University of Houston teaches that foresight is "the multi-disciplinary study of change and its implications in the context of the future. Foresight is not about predicting 'THE' future, but rather about uncovering a range of plausible alternative futures, and then identifying the indicators that suggest the various ways the future is unfolding" (University of Houston, 2020). The concept of understanding how change occurs is central to the idea of foresight and the one that best describes the starting point to investigate threatcasting.

Several well-known categories of foresight methods are widely used in business, government, and military strategy rooms. *Scenario development* creates stories of the future (P. Schwartz, 1991) and is a building block for a more comprehensive study of the future as outlined by *scenario planning* (Bishop et al., 2007). Although he does not explicitly seek after preferred futures, Herman Kahn, thought of as one of the founders of scenario planning, defines a scenario as "a set of hypothetical events set in the future constructed to clarify a possible chain of causal events as well as their decision points"

(Kahn & Wiener, 1967). *Backcasting* explores the feasibility of reaching certain goals and is a major component of threatcasting's framework. Robinson (1990) states,

> "The major distinguishing characteristic of backcasting analysis is a concern, not with what futures are likely to happen, but with how desirable futures can be attained. It is thus explicitly normative, involving working backwards from a particular desirable future end-point to the present in order to determine the physical feasibility of that future and what policy measures would be required to reach that point" (p. 824).

Even the military's *joint planning* method tends to envision future scenarios that the unit would prefer to achieve. For instance, the military end state "is the set of required conditions that defines achievement of all military objectives" (Department of Defense, 2017). The remainder of joint planning seeks to illustrate all the ways and means necessary to achieve the desired end state. Finally, Popper (2008) provides a review of over 25 different foresight methods and many of the circumstances each would be useful. None of them explicitly do what threatcasting does.

Threatcasting takes a different angle: it anticipates strongly non-preferred or undesirable futures, usually stemming from a tightly focused research question, and investigates how we can avoid, mitigate, or recover from these future threats. A "threat," then, is a non-preferred future that, should it come to pass, poses a tremendous risk to *someone's* sense of well-being, livelihood, safety, freedoms, or even existence. In most cases, a future threat disrupts how the world works today, and it most certainly does so in a negative way. A threat could be disruption to the current status quo of daily life, loss of a job, a new product from a competitor, an existential risk to human existence, or anything in between. Threatcasting embraces the ugly side of the future and attempts to investigate systematically how threats in the future could materialize.

In approaching this study, I am making an *a priori* assumption that threatcasting is uniquely situated in the foresight space to provide insights about the future that are not available through other methods. While other foresight methods seek to understand and influence the conditions required to *bring to pass* a desired future, threatcasting takes a different tack by seeking to understand and influence the conditions necessary to *avoid* undesired futures. The difference is subtle, but the two styles of foresight are opposite faces of the same coin. These undesired futures threaten the future in some significant way to at least a particular portion of the population. In this sense, by looking at the inverse of what typical futurists investigate, threatcasting is a necessary complement to the rest of the foresight studies field.

The entire process of threatcasting, as I investigate and describe in Chapter 2, seeks to answer both broad and specific questions about the future. For instance, threatcasting has been a successful foresight tool in academic, industrial, governmental, and military settings. Sometimes future threats pose risks to civil stability, the economy, or national security. Threatcasting has been used to investigate those kinds of threats on behalf of military clients or large banks. Threatcasting can also be used to understand many other threats, such as risks to the future of sports following a worldwide pandemic (Johnson, 2020) or the risks to supply chain management due to the proliferation of automation and artificial intelligence (Johnson & Vanatta, 2018).

My research begins (and ultimately concludes) from an autoethnographic perspective. I seek to understand my experiences in thinking like a futurist and relate them to my professional career as a serving officer in the U.S. Army. Through learning and applying the various steps of the threatcasting methodology to several forecasting

projects, I have come to more clearly realize the power of studying the future and making recommendations for action to decision-makers within my sphere of influence. I will magnify my personal experiences by seeking ethnographies of other futurists who have learned and applied the threatcasting framework to their own studies of the future. All of these perspectives, both mine and those of other threatcasting futurists, should provide me with a little more wisdom about teaching and training other apprentice futurists, which will be part of my job during the next several years of service in the Army.

In order to fully appreciate my journey to becoming a futurist, I need to step away from my personal experience to thoroughly study and understand the nature and processes of threatcasting with sufficient intellectual vigor so that it is translatable to other futurists, researchers, and practitioners. Specifically, I dive deep into the "sausage-making" that happens during the data analysis process after hosting a threatcasting workshop. In threatcasting parlance, this is called *post-analysis* (Vanatta & Johnson, 2019). "The post-analysis consists of multiple clustering and aggregation exercises to determine the patterns in all of the futures modeled during the event" (Vanatta & Johnson, 2019), but what *really* happens during this phase and what are these "clustering and aggregation exercises?" Right now, the literature is void of explanation, making this a perfect place to start a methodological investigation. In this dissertation, therefore, my purpose is to bring scholarly tools to bear to study and understand the processes and theories that underlie the threatcasting methodology, especially the post-analysis process, with the aim of scaling it to a broader population of futurists allowing it to be more appreciated by those new to threatcasting.

Thinking Like a Futurist: Analytics

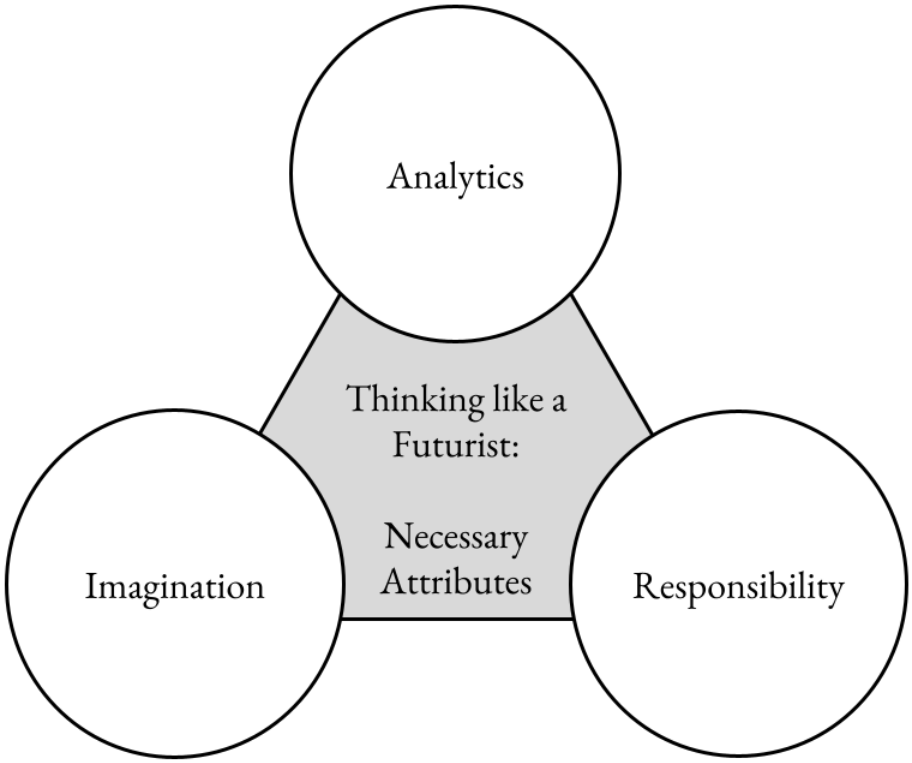
Studying and understanding the processes and theories of threatcasting is best when anchored to a simple frame of reference, and I have developed the triad of analytics, imagination, and responsibility as that referential frame (see Figure 1).

The first of these attributes deals with *analytics*. Analytics is the set of tools, methods, and processes that help the futurist understand how to accurately combine, parse through, and make sense of a substantial quantity of unstructured data created during a threatcasting workshop. I will address my findings on the best practices and processes of qualitative data analysis that helped me make sense of workshop data in Chapter 3 in the section on coding, clustering, and theming. Another important aspect of analytics is knowing what methodological starting point the analyst should adopt when trying to frame the entire project and place its relevance to the questions being asked and anticipated answers. I address an example case of a grounded-theory approach in Chapter 4 and an example case of a hypothesis-driven approach in Chapter 5.

Thus, this dissertation first investigates the strengths and limitations of qualitative methods as they apply to analyzing threatcasting data, including the grounded theory approach and the hypothesis-driven approach. Each of these approaches, and their accompanying coding, clustering, and theming exercises, are appropriate in some projects but less so in others. In comparing the strengths and limitations of each approach, I seek to assist other researchers in choosing suitable analytical tools for the job at hand and demonstrate that threatcasting is a methodology that is flexible to the needs of both the analyst and the requirements of the project.

Figure 1

The "Thinking-Like-A-Futurist" Triad



Note. The attributes required to think like a futurist, or what I call the "thinking-like-a-futurist" triad, include analytics, imagination, and responsibility.

Brian David Johnson, the Threatcasting Lab director at Arizona State University, developed his way of analyzing workshop data through a career in microchip development and engineering at the Intel Corporation. His methods have a long tradition of success in industry and business and have also been used in answering research questions for government and military organizations. Threatcasting follows a consistent set of steps that look at social, economic, technological, cultural, and historical trends,

projects them out a decade into the future, and develops a story, or scenario, that vividly captures how a person might experience these trends as they change over time into a threat. To investigate both the threat and the potential solutions in the threatcasting way requires data, often in the form of stories or scenarios, that describe a person, in a setting, experiencing that future threat.

Despite being a methodology that has been developed and fine-tuned over the last two decades to aid practitioners and those who are in the position to make decisions about the future, the academic literature on threatcasting is sparse. Yet, there is a wealth of expertise to draw from to demonstrate that the methodology is both practically and academically grounded. Sociology, education studies, science and technology studies, and other disciplines that use narrative analysis, inductive analysis, and other styles of qualitative studies have refined and honed processes and theories that will only contribute to the advancement of threatcasting as an art and as a science.

How does the threatcasting methodology lean on established practices of qualitative data science to become a more academically grounded methodology? How can futurists become more proficient at analysis and come to conclusions in a more rapid, consistent, and thoughtful manner? These questions can only be answered by studying the techniques and processes of qualitative sciences, seeking new methodologies that span interdisciplinary fields, and then practicing and testing them in various ways.

While most analysis of raw threatcasting data tends to reveal generalizable actions, it takes a very keen eye to uncover when a threat in the future is unprecedented and thus requires special attention and action. Sometimes these findings are early indicators of black swan events (Taleb, 2009). Other times, they may appear outwardly

ridiculous at first (Dator, as cited in Candy, 2010), yet have a much deeper, perhaps sinister, truth to them that is no laughing matter. In any case, pure analytical horsepower, regardless of its precision, cannot produce conclusions that mean much to address the complexities of future change. A futurist also needs to lean into the rest of the thinking-like-a-futurist triad for answers.

Thinking Like a Futurist: Imagination

The second attribute of thinking like a futurist is *imagination*. The most challenging part of post-analysis is arguably understanding the concept of novelty or knowing when the analyst has found a genuinely unprecedented future threat that decision-makers are not yet prepared to address. The most novel assessments of the future, those that are low probability yet high impact, are the gems of analytical work - elusive to discover. Their appearance is often obscured when found, and it takes precise cutting and polishing to make them stand out. The attribute of analytics suggests there are tools to collect, processes to practice, and methods to follow that guide the analyst from raw data to the final product. Yet, it is the attribute of imagination that envisions how these analytical gems will look in their cut and polished end state.

I believe that the most noteworthy contribution this dissertation makes is an investigation of the nature of novelty, which at its core is an expression of imagination. I explore how it is defined and used within the threatcasting framework, why it is such a powerful category of research findings, some examples of novelty from previous threatcasting reports, and ultimately, why the concept of evolutionary novelty illuminates

the path to becoming a better designer of the future. I tackle this multi-faceted concept in Chapter 6 and investigate its ties to responsible design coupled with the value of personal experiences in Chapter 7.

In addition to being a unique and gem-like analytical finding, the term "novelty" also describes the third round of data analysis that aggregates and synthesizes the previous rounds of analysis as Vanatta & Johnson (2019) teach it. The ultimate holy grail for the threatcasting futurist is finding the one or two synthesized ideas that span across many of the raw and unpolished scenarios written in quick brainstorming sessions and that have impactful meaning to the readers. My research formalizes threatcasting's understanding of novelty (in all its uses) and synthesizes the best practices of qualitative data analysis and creative insight techniques to help the analyst find "it." Thus, the second aim of this dissertation is to further explore, define, and help futurists understand what novelty is, how to find it, if it exists, within the data of a particular project, and help make sense of its impacts on the project and larger readership.

Thinking Like a Futurist: Responsibility

The final attribute a futurist needs to adopt is *responsibility*. Responsibility takes many forms within a threatcasting project. Built into creating and implementing a threatcasting project plan is the underlying obligation to the project sponsor. Every threatcasting project starts with a foundation, including a narrowly bounded topic, specific research questions, and application areas that the sponsor will likely need to make resource and policy decisions on (Johnson, Vanatta, et al., 2021). Responsibility to

the client requires part of the output of a threatcasting work session and subsequent post-analysis effort to be a list of practical and achievable action items. The expectation is that the client and other gatekeepers will use these action recommendations for policy and resourcing decisions, inputs to wargaming and other planning processes, or discussion items in board meetings and executive decision rooms.

Responsibility to the client is only part of this attribute, however. Responsibility to human values, long-term sustainability, balancing ethical and moral tipping points in the future, and overall being a good person are some of the other aspects of responsibility that futurists must consider while doing their work. Without principles of *responsible research and innovation*, *risk governance*, and *adversarial design*, futurists run the risk of recommending futures that only benefit part of the population while continuing to marginalize groups without a voice. It is a weighty calling to consider how far-reaching one's analysis and recommendations will travel. Without seeming trite, a true futurist must examine and understands the future impact of their work. I connect the responsibility attribute to other factors of responsible design in Chapter 7.

Developing the idea of the thinking-like-a-futurist triad was itself the culmination of personal reflection and observation of other futurists at work - in essence, a meta-approach of applying analytics, imagination, and responsibility. As an apprentice to Professor Johnson for two years, I have come to recognize that he intuitively finds meaning and novel connections among workshop data based on his experience and personal views of the world. But finding these connections in the same way did not come quite as quickly to me. In other words, his intuition and his way of thinking were not my way of thinking. This raises the question of who is right, or rather, is there a "right" way

to do threatcasting? More importantly, is the analysis and interpretation of the data a product of the analyst or driven by the problem set and the client's needs?

Despite my efforts to follow Professor Johnson's analytical processes, I struggled to reach the same conclusions and findings. Not arriving at the *same* conclusions bothered me for quite some time. Using a process-driven approach, I figured that I could take the same data inputs as the next person, apply the same processes, and come to a reasonably similar set of outputs. Not exactly. To say that threatcasting (especially the post-analysis phase) is just a process disregards and over-simplifies the importance of imagination and responsibility to other people. The worldviews and biases of each person involved in the threatcasting process, from project conception to scenario development and then to analysis and publication, are necessary to elevate threatcasting beyond a simple analytical exercise. Embracing this individuality is a feature of threatcasting and not a bug! There is no bias to squash in threatcasting. Instead, I needed to understand how to temper and understand what tendencies are present and how these are meaningful inputs to the process that genuinely influence the final interpretation. Thus, I began a lengthy conversation with many futurists and a quest to understand the art of analysis just as I also sought to understand the science of analysis and ultimately led me to develop the thinking-like-a-futurist attribute triad.

This meant I had to find some way to help me understand my personal analytical skills, discover gaps in my analytical science, and better understand how to coordinate and account for other analysts' inputs working together on a project. As I read and studied the processes of qualitative methods, especially in the social sciences, I recognized there were terms, concepts, and ways of parsing through data that resonated better with me and

described the things Professor Johnson was doing in different words. For instance, I noticed that Johnson uses the idea of "finding meaning" as the second step in data analysis (Johnson, Vanatta, et al., 2021), yet this corresponds with a whole set of skills such as coding, clustering, and theming that only made sense to me when I applied these concepts from a background of qualitative data analysis. Tying Professor Johnson's years of practice with theoretical frameworks and practical skills is the next logical step to formalizing threatcasting as a practitioner's tool by grounding it in a rigorous analysis of approaches and processes.

By the end of this project, I will demonstrate that the analyst and their worldviews, biases, and unique experiences make finding novelty possible and that discovering novelty is a uniquely human trait. Someday, it may be possible for a machine to conceive future threat scenarios. Another device may provide in-depth analysis that rivals a human futurist in trend prediction, indicator awareness, and policy recommendations. Still, a proper understanding of how a future threat will change humanity cannot occur without the human attributes of imagination and responsibility.

This leads me to this dissertation's final aim: to reveal new and impactful insights into becoming a threatcasting analyst and thinking like a futurist. Through my journey that started as an apprentice futurist and emerged as a seasoned analyst leading my own research projects, I demonstrate that finding novelty is possible only by merging sound scientific practices and artful application of biases and experience, and the intangible effect of working with people. Threatcasting is a people-centered process and should have a people-centered reason for doing it. A personal journey via autoethnographic means is essential to this study because it scrutinizes the adaptability of the threatcasting

methodology to many styles of inquiry, provides evidence for thinking like a futurist, and scrutinizes the culture of threatcasting. Because each analyst's approach can illuminate different conclusions within a project, there is also the art of mixing and matching dissimilar analysts within a project that can complement each other's practices. By drawing upon skills from the qualitative sciences, I also hope to clearly show that preparing for the future shock can be improved with a purposeful study of how to think like a futurist and by enhancing the attributes of analytics, imagination, and responsibility.

CHAPTER 2

METHODS AND APPROACH

To review, the purpose of this research is to bring scholarly tools to bear to study and understand the processes and theories that underlie the threatcasting methodology, especially the post-analysis process, with the aim of scaling it to a broader population of futurists and allow it to be more beneficial to those new to threatcasting. This section introduces the "analytics" skill set and the methods or approaches used in investigating threatcasting's processes and theories. Similarly, the case studies in Chapters 4 and 5 demonstrate two ways to use analytics to answer a threatcasting project's research questions and move along the path towards the "imagination" focused discovery of evolutionary novelty.

I use three approaches to investigate the processes and techniques of post-analysis and relate them to how to think like a futurist. First, I use a *comparative case study approach* to compare and contrast two cases using different techniques: a grounded-theory method and a hypothesis-driven method of analysis. Both the exploratory and comparative case study approaches aim to methodically uncover ways to seek for and illuminate novelty from the data. Although these are only two of many possible paths to frame the entire analytical undertaking, I focus on grounded theory as the baseline for threatcasting's post-analysis process. Grounded theory is the closest explanation for Professor Johnson's series of analytical steps developed over the past two decades.

On the other hand, hypothesis-driven analysis is a new approach to threatcasting analysis. It is relevant because it corresponds to the idea that a threatcasting project is always trying to reach a detailed understanding of the future and from a certain point of

view. Our project's hypothesis on the future of extremism establishes a theory of identity and radicalization then attempts to validate conclusions using threatcasting data. This is also the first time a hypothesis-driven approach has been used in the threatcasting methodology and documented in the literature. Thus, I can compare these two approaches for their strengths and weaknesses and provide a perspective on when they are appropriate (or inappropriate) for meeting the aims of a threatcasting project.

Second, I use an *exploratory approach* to determine how current futurists trained in the threatcasting methodology think during post-analysis. I suggest that futurists use some personalized variation of data coding, clustering, and theming to develop their findings for a threatcasting problem set, but they may not use the same terms to describe what they are doing. How each futurist navigates the steps of summarizing, finding meaning, and finding novelty varies because of backgrounds, biases, and life experiences that shape how specific ideas resonate and cluster together. This approach reveals how differences in life experiences, world views, opinions about responsibility, and imagination augment rigorous and scientifically backed analytical tools to form a better understanding of future threats and how to avoid or better prepare for future shock.

Third, I use an *autoethnographic* approach to investigate and reveal how my personal experiences of moving from an apprentice futurist to leading my own research projects provide insights into strengthening my ability to think like a futurist. While I lack the experience and skill levels of my mentor, Brian David Johnson, there is value to new futurists in relating the struggles and successes I have experienced learning and applying qualitative methods. As each analyst must develop their own style and approach to the post-analysis process, no two journeys from apprentice to expert will ever be the

same; some techniques will resonate clearly, and some will make the analyst's mind muddled and their results unclear. Thus, developing one's individual approach to threatcasting will necessarily be a journey of experimentation, rejection, and adoption. Yet, in all cases, the analytics-imagination-responsibility triad will be evident throughout this journey.

Lastly, I summarize my findings of the above-mentioned methodological approaches to argue that finding novelty (in all its various forms) reveals one path to responsibly designing a better future. I believe that hyper-novel findings are the rare nuggets of future study that help us avoid, or at least come to grips with, future shock, but this is only one perspective of what novelty is, what it means to find it, and how it can be applied to the aims of a threatcasting project. This argument will ultimately discuss what it means to use the techniques and findings from threatcasting to define responsibility for the future and discuss what "better" means and who gets to decide that standard of measurement. In the following sections, I will discuss how I intend to dissect different ways of understanding novelty and how this links to analytical methodologies, imagination, and the essence of responsible design.

Comparing Grounded Theory and the Hypothesis-Driven Approaches

The first analysis I conducted compares the grounded theory approach and a hypothesis-driven approach that uses case studies from two different threatcasting workshops. The grounded-theory case study demonstrates analytical techniques I used while working through the data on a project investigating the future of weapons of mass

destruction and cyber (Johnson, Brown, et al., 2021). I assisted Professor Johnson with analytical duties and generally followed the traditional post-analysis steps described in Chapter 3. In Round One (summarizing), we scanned through the models and coded for gates, flags, milestones, and vulnerabilities as categories and then did a first-pass coding analysis for early insights. In Round Two (finding meaning), we finished coding analysis and developed clusters and groupings of ideas that fell under like-themes. Finally, in Round Three (finding novelty), we discussed and agreed upon unique, thought-provoking, and meaningful conclusions that became the core elements of our reportable findings on the future threats of WMDs and cyber.

Next, I used the hypothesis-driven approach to investigate threat futures of extremism and insider threat within the United States in 2031. Data for this method was collected during a workshop held in October 2020 and was combined with data from five previously published threatcasting reports. The extremism workshop had participants from the Undersecretary of Defense for Intelligence & Security (Insider Threat) office, the Army Cyber Institute, the ASU Center on the Future of War, and various academic, government, and industry organizations. The hypothesis part of this approach was a theory about extremist recruiting and the narratives used to either 1) move a person in a trusted position to a fringe or extremist point of view or 2) move a radical idea from the edges of acceptability to a more central and recognized point of view, thereby becoming more accessible to a larger audience.

For the extremism analysis, I am grateful for the assistance of Josh Massad, another Ph.D. student training with the Threatcasting Lab, and for Renny Gleeson, a fellow at the Lab. We began our study with two frameworks from previous research: one

framework described a set of narrative constructs that motivate and influence people's identity. The other framework described a list of radicalization risk factors present in extremist and terrorist recruitment and radicalization programs. We filtered and selected scenarios developed during five previous threatcasting workshops conducted between 2017 and 2020 for markers of extremism, recruitment, insider threat, or narrative warfare. Additional scenarios generated during the extremism workshop completed the data set. We initially used hypothesis coding (Saldaña, 2016) and then pivoted to other best practices of qualitative data analysis to test whether the theory of extremism and recruitment will still hold in the next decade.

The strengths and weaknesses that appear with grounded-theory and hypothesis-driven models of analysis are not measured on the same scale. They each are appropriate for different types of research questions. Since the grounded-theory approach is the basic technique in threatcasting post-analysis, the findings from this research do not overturn years of practical experience. Instead, by naming, describing, and clarifying the three-round post-analysis process, I submit that threatcasting is grounded in sound and rigorously validated practices and should be considered a viable method for evaluating future threats. I also demonstrate that the hypothesis-driven approach is appropriate in some contexts and should be regarded as an optional technique for upcoming projects. By showing how we maneuver through this latter approach, I believe that threatcasting can open up to a broader field of research questions than government and military-focused threats. I also show the applicability of re-using threat scenarios as data points in different contexts, thereby emphasizing the interconnected nature of all the complexity required to create visualizations of the future.

Grounded Theory Analysis

Analytic induction as a method began in the 1930s to attribute causal explanations to phenomena in the social sciences, as opposed to empirical evidence in the natural sciences (Smelser & Baltes, 2001; Znaniecki, 1934). When using the logic of analytic induction, the analyst first creates a hypothesis about the data that they want to explore, observes data, and then generalizes their conclusions to develop a set of principles that are probably true given the observations. For example, if I were studying how extremist actors and narrative identity interacted in the next decade, I could say that someone we might label "an extremist" is not satisfied with their current identity as described by the dominant narratives of their culture and seeks after sympathetic narratives that reflect their desired identity. This would be my hypothesis that I would need to support with data. After researching and generating data, I might later conclude with a generalized principle, such as people who have an unsatisfied identity crisis and a grievance against the government that cannot be resolved through legal or administrative processes may feel they have no choice but to resort to violence to rectify the dissonance between their personal identity and the expectations of being a good citizen. In fact, this is one of the generalized conclusions we found in our workshop on the future of extremism in America that I illustrate in Chapter 5.

If the analyst finds something in the data that does not clearly fit the hypothesis, analytic induction suggests there are two choices: 1) alter the hypothesis on the fly - the idea of a running hypothesis works here - or 2) limit the range in which the hypothesis explains the generalizability of the observations (Robinson, 1951). This means we can

decide in which circumstances the hypothesis applies and in which it does not, thereby giving the analyst another indicator of possible novel situations. Suppose the analyst chooses to alter the hypothesis. In that case, they might lean on the techniques and processes of grounded theory to rewrite the hypothesis to describe what the data are indicating to be true. If the analyst chooses instead to limit the generalizability of the hypothesis instead, then they could conclude that the hypothesis only applies in certain situations and not others and clearly indicate those boundaries. In either case, induction allows us to create generalizations and conclusions from a set of observations.

As a close cousin to other inductive methods, grounded theory application is a commonly used qualitative method seeking to find certain generalizations from specific examples or observations (Corbin & Strauss, 2012). The benefit of using grounded theory models in threatcasting post-analysis is that these models are heavily dependent upon good coding, categorizing, and theming skills. The process to do this analytical work is trainable.

The added benefit of drawing upon grounded theory best practices allows the analysis to naturally self-organize into intermediate and final conclusions that support the research questions. Charmaz (2000) uses grounded theory methods to make "inductive guidelines for collecting and analyzing data to build middle-range theoretical frameworks that explain the collected data" (p. 509). Another way of saying this is that examples from the data link together to make a framework from which the researcher can draw conclusions and build a hypothesis that explains why *those* particular circumstances induced *that* specific effect. Grounded theory also self-corrects throughout the data collection process and strongly emphasizes comparative methods (Charmaz, 2000;

Corbin & Strauss, 2012). For threatcasting, that means that the analyst will create categories, themes, and early conclusions soon after reading through the first couple of scenarios. We should expect the analyst to continue to modify those categories and themes throughout the entire post-analysis process until there are no new data that would alter the conclusions.

In threatcasting, we want to find novel ideas outside the universal. We want to know when the current hypothesis (in the present) will not hold up for conditions in the future. But first, we need to ensure that our hypothesis (or theory) contains as many necessary (but not always sufficient) conditions for explaining the future. Only when we have identified the boundaries of the theory as closely as possible, do we look for outliers that cannot be explained by our current (and highly modified) theory. We also need to remember that our theory is "grounded" in the data itself. This might indicate novelties that are worth taking into account in our analysis. It might also indicate an interplay between analytic induction and grounded theory until we get to the limits/boundaries of our theory.

Hypothesis-Driven Analysis

An alternative way to approach threatcasting data is to bring a hypothesis that explains why something appears to be true in the present and test it against scenarios that describe a different set of circumstances from the future. If observations from our future scenarios continue to validate the hypothesis, then we should be able to recommend courses of action to avoid, disrupt, or mitigate the effects of a threat as it begins to

manifest over time. A hypothesis-driven approach can start with a predetermined set of codes, categories, and themes derived from a present-day assessment of a threat that predict what should appear in the data set (Saldaña, 2016, p. 171). If the ideas appear in our future scenarios, we can reasonably conclude that the threat will likely manifest in the same way it displays today.

If the threat is not observed in the same way, the analyst can then choose to find more data points or begin to adapt the hypothesis as they would for a grounded theory investigation. Either way helps visualize the boundaries of a problem set and identifying novel ideas that refuse to be easily corralled. Chapter 5 presents an entire case study that began with two interwoven frameworks of narrative identity and radicalization risk, which provided us our starting point from which to interpret our data. We coded and categorized the data according to our predetermined frameworks. Then we assessed whether present-day political, social, technological, and environmental conditions could change over the next decade to meet the conditions the frameworks suggested would be necessary to make our conclusions about the future of American extremism valid.

Coding and Qualitative Data Processing

To accurately and repeatedly assess data with few errors, the analyst needs to understand the processes and techniques of data coding, even if they do not know it is called coding. Coding is the process of interpreting and attributing meaning to ideas within the corpus of data (Saldaña, 2016). We can assign illustrative phrases such as "biology is programmable" or "scaring as a tactic" to ideas of how a threat appears in a

particular (fictional) person's scenario. This provides the analyst with a creatively described concept that could lead their eyes to pick out a similar occurrence in other scenarios.

It is relatively standard in qualitative research studies to code data multiple ways in the same project, each time looking for different angles. For threatcasting, I find that *in vivo* coding (assigning codes by using direct words or quotes from the text), process coding (describing actions by using "-ing" words), and concept coding (describing ideas instead of objects) provide functional divisions during the first cycle of analysis. Concept coding of the commonalities between gates, flags, and milestones allows for a robust horizontal clustering between the action items suggested by the models.

Clustering allows the analyst to group similar codes and begin seeking more generalized categories of ideas. Theming enables the analyst to draw initial conclusions and give a name to ideas that span multiple threat futures and provides the analyst with the first opportunity to glimpse one definition of novelty. In this case, novelty means something that does not fit within the rest of the data or falls outside the hypothesis. Sometimes this is called an outlier.

The strength of coding, clustering, and theming comes not from a mechanical evaluation of the data but rather from applying forms of induction (or moving from specific observations within the data to a generalized hypothesis) and letting the data "speak" for itself. Choosing which phrases or ideas to code and why they seem essential takes multiple turns through the data. Picking out what a code should be is part of the art of analysis but can be trained. It also comes easier with practice.

Exploring How Analysts *Think* They Think

For the exploratory approach, I used a data set of three modified scenarios that tested how individual futurists differ in their personal strategies to elicit meaning and novelty from the same data. The key to this test is finding what ratio of analytics, imagination, or responsibility governs each phase of post-analysis and whether the ratio changes between phases. Because analytics, imagination, and responsibility are subjective categories and there is no concrete scale, I will rely on a combination of self-reported ratios and a qualitative assessment of two separate engagements with my participants.

In order to gather data on how futurists think, I used scenarios modified from an unpublished workshop about the future of post-pandemic public health to query the minds of four experienced threatcasting analysts. I asked participants to record a "talk aloud" session reviewing these scenarios in a standard post-analysis workflow. Participants were asked to modify the summary, extract themes that provide meaningful insights across all scenarios, and identify novelties that emerged. These emergent novelties would likely appear as either outliers or evolutionary novel findings. I was interested in querying *how* the analyst recognized whether they could identify critical moments in their thinking that helped them solidify their findings.

I then followed with an interview lasting approximately 60 minutes with each participant. In these interviews, I had each participant walk through their analytic tools, creative processes, and principles of responsibility to discover if there were still some ideas not used in the "talk aloud" session that might reveal more about how they

connected certain data. This interview was also an opportunity for each participant to see themselves from an external perspective and then reflect on how their own processes affected how they interpreted data. Essentially, I provided an analytical "mirror" for each futurist to understand better their own biases, worldviews, and analytical strengths and weaknesses. Some participants immediately recognized the mirror, while for others, it was more subtle. I believe that regular self-evaluation and reflection provides an opportunity for the futurist to see how they use analytics, imagination, and responsibility in their work. If one leg appears lacking, a self-reflection mirror might be the punch in the arm needed to balance out their thinking.

To quickly compare data in a manageable format, I used Temi, an automatic translation software service, to transcribe the "talk aloud" and interview sessions. I coded and analyzed the transcripts for recurring themes. Since I had no previously developed hypothesis to prove or disprove, I used grounded theory techniques to identify common themes between participants, cluster common themes together, and draw conclusions about the trends that appear. Several coding techniques illuminated my interviewees' tendencies and thought processes, including process coding, concept coding, values coding, and *in vivo* extracts (Saldaña, 2016).

Since I worked from a small pool of analysts who all have been trained by Professor Johnson, I expected (and found) commonalities between the participants' techniques. Still, there were fascinating and valuable differences that transcend the effects of training. These individualities illustrate how life experiences and personal paradigms color our ability to analyze with perfect objectivity. Reiterating an earlier point, I submit that the threatcasting process celebrates and is looking for these variations

in processes because the strength of insights into the future comes from diversity rather than from numbly following the crowd or mechanically applying techniques to data, expecting that a solution will present itself automatically. This also gives evidence that analytics alone cannot make a good futurist. A healthy dose of imagination tempered by responsible design practices is also necessary.

Designing the Future with Threatcasting

Finally, I concluded my research with an investigation about the contribution that threatcasting has for forecasting and the field of responsible innovation and design. I discovered that responsibility, the third leg of the thinking-like-a-futurist triad, was the least visible. It did not consciously enter into analytical decisions until I purposefully asked how responsibility was tied to personal analytics and imagination. As soon as I identified responsibility as a critical component to thinking like a futurist, all the people I tested with the talk-aloud scenario and interview process immediately agreed that their work was intended to shape the future in precise ways and responsible design principles could inform their personal analytical strategies. This indicated that responsible design principles could be trained and exercised just like sound analytics principles, which is not something the threatcasting framework has previously acknowledged or consciously practiced.

To further discuss the importance of responsibility in thinking like a futurist, I present ideas emerging from design and futures thinking, technology innovation, and socially responsible innovation to explore what it might mean to be “responsible

architects" of a "better future." Those that investigate the future with the eyes of a threatcasting futurist are called upon to make judgments about defining threats in the future, the sequence of events to that future, and the steps that gatekeepers can take to avoid, recover, or mitigate the threat. It is a heady responsibility, and this discussion will reflect the power and privilege that comes with being a threatcasting futurist.

This discussion includes the notion of what it means to be successful when applying the methodologies of threatcasting. Success in the method means that the recommendations for action outlined in a final project report truly meet the aims previously identified in the threatcasting foundation and are feasible responses to the threats outlined in the analysis, even if they are hard to do. Thus, a successful project provides meaning to those who use the results to take action. In addition to providing a sort of moral compass for the threatcasting analyst, responsibility is also an attribute for those who have the onus for action. The gatekeepers, policymakers, and those who must enact the changes necessary to avoid, mitigate, or recover from a threat in the future are who I consider to be the real architects of the future. How they implement policies and carve out resources must also be done responsibly and sustainably; else they risk triggering other threats and other undesirable futures.

My Journey from Apprenticeship to Expertise

The final approach in my methodology is an autoethnographic look at the growth and maturity I gained while maturing from an apprentice futurist to leading my own team of analysts on a timely and highly controversial topic. More precisely, I weave my personal experiences as a way to illuminate and view the people and culture of

threatcasting. Ellis & Bochner (2000) refer to this as a reflexive ethnography, one in which the researcher's own experiences are studied along with other subjects. As I focus on personal experiences, I do so only to illustrate "how I did it" rather than as a "how-to" become a futurist. These experiences include discovering the importance of Phase Zero planning and curating the right people to be a part of a threatcasting project; experiencing first-hand the "ah-ha!" moment of recognizing a hyper-novel finding; the gut-wrenching decisions to publish and stand behind controversial and potentially upsetting conclusions about the future of America and the rise of extremism; recognizing and honoring the valuable and often cross-wise opinions of a strong-willed analytic team; and the development of the futurist's attribute triad.

I found it best to write about my growth and experiences horizontally across this entire dissertation rather than restraining it to one particular chapter. This allows me to present my findings on the subject, whether it was the threatcasting process itself or a case study using a specific approach, and then illuminate the culture of threatcasting and the people who make it happen through commentary on my experiences. For example, in Chapter 4, I present the technique of "memoing" or pausing to record why specific codes and clusters are meaningful to me to return to them later to find additional insights into the data. I can only present the memos I have recorded and comment on the connections I saw in the data. This is because, as far as I can tell, I am the only threatcasting analyst to purposefully, albeit sporadically, use the memoing technique, and I share some thoughts as to why this may be. Perhaps in the future, other analysts will become more reflexive and use memoing more frequently, but for now, I can only provide insights into how they helped me.

This study purposefully pulls from several traditions of qualitative science. Still, it does not advance the literature in any fields such as sociology or ethnography, nor does it extend the knowledge of any inquiry methods in those fields such as thematic analysis or grounded theory analysis. However, it uses these methods quite extensively. That is not its purpose, nor should this work be judged on those merits. What this study does instead, is investigate, dissect, and understand the principles and practices of how and why threatcasting borrows methodologies and adapts best practices from foresight sciences, analytical traditions, and responsible design to deliver reports on how to imagine and respond to future threats that no other methodology in use can do. This study investigates every aspect of threatcasting, from project conception and participant curation to data collection, data analysis, and report publication, to make the processes and frameworks accessible, repeatable, and adaptable to veteran and novice futurists alike.

CHAPTER 3

PROCESSES OF THREATCASTING

In this chapter, I briefly review threatcasting as a practice as currently described in the academic literature and add additional observations about the processes and methodologies missing from the literature. This provides us with the necessary vocabulary and concepts of threatcasting to develop the argument that threatcasting is uniquely situated in the forecasting space to provide insights into the threats of change that no other methodology currently does.

One of the specific areas of threatcasting that I focus on for the remainder of this study is post-analysis. Post-analysis is the data analysis phase of threatcasting using a set of original techniques developed by Brian David Johnson over several decades. In order to examine post-analysis in-depth, critique it for thoroughness, and adapt it to my needs as an analyst, I draw on the qualitative sciences introduced in Chapter 2 as the baseline of analytic techniques necessary to understand and apply post-analysis. I mainly use theoretical frameworks for coding, clustering, and theming techniques; grounded theory, analytic induction, and exploratory approaches to qualitative data analysis; and hypothesis-driven analysis theories as best practices of post-analysis. I then conclude with several approaches to defining and finding evolutionary novel conclusions and unique outliers that do not fit within grounded or hypothesis-driven theories and why futurists might need to give them special attention.

Before I begin investigating threatcasting, I first make an *a priori* assumption that threatcasting is uniquely situated in the foresight space to provide insights about the future that are not available through other methods. Included in this assumption is the

notion that threatcasting *works* and is valuable beyond the academic achievement of publishing a report. To illustrate this point, I highlight two instances of public threatcasting reports being used by organizations to explore unique threat futures.

In 2016, the Army Cyber Institute at West Point conducted a workshop exploring threats about increased automation and the attack vectors automated appliances and Internet-of-Things devices would create (Johnson, 2016). One model developed during the workshop imagined misbehaving refrigerators that sent out automated requests for milk on a scale that forced industrial supply chains to automatically reprioritize the shipment of perishable goods over less urgent items. One of these de-prioritized shipments contained repair parts needed to bring a New York City port's radioactive detector back online. As a result, enemies of the United States were able to use a window of opportunity to smuggle a dirty bomb through the compromised and unmonitored port and detonate it in New York City to catastrophic results.

This scenario intrigued executives at Cisco's Hyperinnovation Living Labs (CHILL). They contacted Brian David Johnson to develop it in more detail and create a graphic illustration of how the new technologies of the model would be used to "explore the dark side of inaction as well as the upside of solving tough challenges" (Johnson & Winkelman, 2016). The resulting graphic comic, "Two Days after Tuesday," informed subsequent planning sessions with senior executives from Citibank, Cisco, D.B. Schenker, General Electric, and Intel to imagine "increasingly hardened prototypes" that would address the vulnerabilities of this threat (Johnson & Winkelman, 2016, p. 2).

A second similar example comes from the Army Cyber Institute's 2017 workshop on the future of weaponized artificial intelligence (Johnson et al., 2017). Participants in

this workshop developed 23 effects-based models imagining the worst of what enemies of the United States could throw against it by using artificial intelligence as a weapon. Some of these models were later reimagined and developed into science fiction prototypes with detailed illustrations to train and educate the military workforce. These prototypes showed how AI and cyberattacks might be used to compromise military supply chains (Johnson, Winkelman, Burchielli, et al., 2018), cascade into lethal attacks against US tanks and combat vehicles (Johnson, Winkelman, Hudson, et al., 2018), or change the nature of clandestine spycraft (Johnson, Winkelman, Buccellato, et al., 2018). Although subsequent planning and development based on these threatcasting models remain behind the secret walls of military installations, there is no doubt that senior military leaders were witnessing visceral illustrations of how threats could play out in the near future. The fact that Arizona State University's Threatcasting Lab has enduring and continuous relationships with the Army Cyber Institute at West Point, the F.B.I. and the U.S. Secret Service, as well as other U.S. government organizations, suggests that threatcasting methodologies are and will continue to be critical tools for continuing to imagine and prepare against these threats.

Threatcasting Overview

Vanatta & Johnson (2019) write about threatcasting in an overview published in the *Journal of Defense Modeling and Simulation*. They state that threatcasting has four phases. These phases are research synthesis, futurecasting, time-phased alternative-action definition, and synthesis and final report (Vanatta & Johnson, 2019). The four phases are briefly summarized below, but shortly after this summary, I show more depth to these

phases that should be explained and an additional critical phase that precedes the entire process.

In Phase One, futurists initiate research synthesis with prompts derived from background research, interviews, and subject matter expert estimations. These prompts are developed during Phase Zero, which I will discuss in detail shortly. The remainder of Phase One's research synthesis often occurs during an on-site or virtually distributed work session, also called a threatcasting workshop - I use the terms interchangeably. Research synthesis allows participants to review the research inputs, receive perspectives from subject matter experts, and resolve unclear terms, definitions, or expectations at the beginning of a work session. Combining expert knowledge with their own knowledge, experiences, and expertise allows participants to have both a common understanding of the problem at hand and unique angles to tackle the next phase.

In Phase Two, workshop participants break into teams of three or four people and begin futurecasting to create models of the future threat. Futurecasting is when participants imagine a person in a place, experiencing a threat, and creatively develop the environment, the conditions, and perhaps the reactions and emotions of both the protagonist and the threat actors. This phase produces effects-based models that envision what participants want to avoid happening in the future (Bennett & Johnson, 2016). In this phase, we do not look for how the threat materialized or what actions should be taken in response but rather focus on the effect the threat has on a person. In particular, the model might contain a snapshot in time that describes a person, in a place, experiencing how the threat manifests. We are interested in modeling the effects of that threat, how it

feels to the person, what impacts it has on daily life, and ultimately how the threat is seen as a Tofflerian "shock" to everything we anticipated the future to be.

Phase Three is a mouthful: time-phased, alternative-action definition (TAD). TAD simply engages several "backcasts" that work backward from the time of the threat event to the present to identify critical moments in which something might be done to disrupt, mitigate, or recover from the effects of the futures modeled in the futurecasting phase. TAD is often referred to as the backcasting phase, as it also draws on the wealth of literature available in this field (Dreborg, 1996; Quist & Vergragt, 2006; J. Robinson, 2003). Backcasting also begins shaping responses to one of the essential requirements of the threatcasting foundation, the application areas.

Finally, Phase Four, or synthesis and final report, is when the analyst earns their keep. This phase, often called post-analysis, summarizes the models, filtering for common themes, clustering ideas together, and ultimately relating the findings to the threatcasting foundation, including the research questions, and linking them to practical applications. There is very little literature on what happens during Phase Four. This is one of the primary reasons for this study - it takes a certain amount of savvy, creativity, and experience to tie theoretical models (made through imagination and a bit of science fiction) to practical applications that need to be sequenced and resourced over time to ensure that our threat futures can be avoided, mitigated, or recovered from.

Phase Zero: Threatcasting Foundation, Subject Experts, Participant Selection

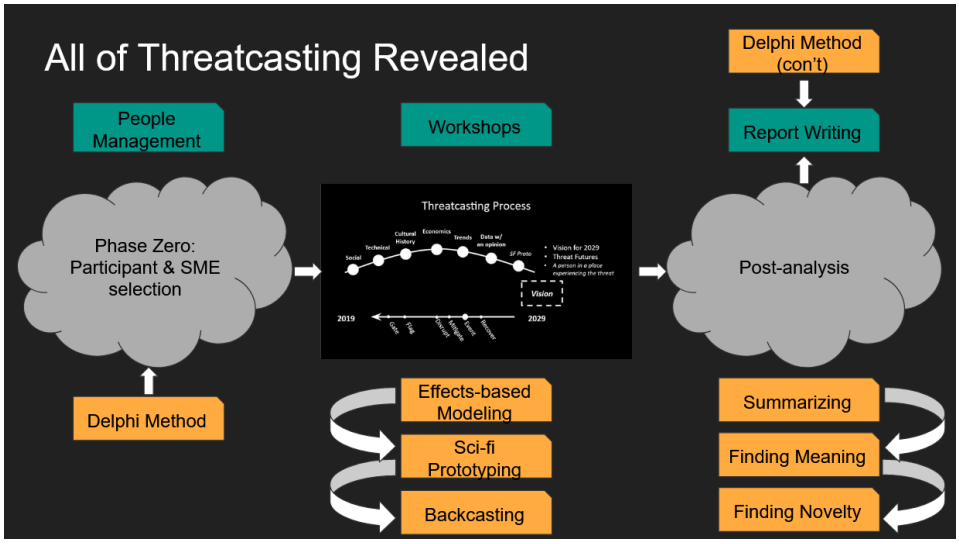
In addition to the four phases outlined by Vanatta and Johnson (2019), I have discovered a substantial Phase Zero that is not in the authors' overview, preceding the four-stage threatcasting model (see Figure 2). I found Phase Zero to be equally as important as the data collection and post-analysis stages, as it requires the analyst to think critically about the threatcasting foundation.

The threatcasting foundation includes three boundaries that must be set before any data collection, subject matter curation, or other planning events. The foundation consists of 1) the topic area under consideration and the boundaries for defining what part of the topic is included and what is excluded; 2) an answerable research question to narrow down potential pathways of inquiry on the selected topic, and more specifically, what the project will seek to uncover; and 3) understanding where and how the findings of the project will be applied, also called the application areas. This is the part when the analyst begins preparing the "so what?" and "who else needs to know?" about the information that the rest of the project will aim to answer.

Phase Zero includes the mindful selection and invitation of workshop attendees who will create the raw data and future scenarios necessary to understand the probable palette of threat futures better. Attendees should reflect the wisdom of practitioners in the field being studied and mirror the cultural, intellectual, racial, and gender diversity that the future requires.

Figure 2

All of Threatcasting Revealed



Note. This image displays all the phases of threatcasting, including Phase Zero: Participant & SME selection and Phase Four: Post-analysis. The center "Threatcasting Process" box adapted from Vanatta & Johnson (2019), used with permission.

Although Phase One talks about synthesizing the expertise of subject matter experts, there is no additional information about how that happens. The hard work of this synthesis begins in Phase Zero. This requires choosing prompts, or short questions to consider, that set the stage for what topics might be included and what ones are probably not relevant. For example, in a workshop investigating the future of extremism in America, I developed a prompt to consider the industry response to extremist content by asking questions such as,

1. How should the social media industry respond to the friction between intervention and business models (e.g., profit)?

2. In an era of partisan politics, what is the line between extremist content and mainstream media?
3. How do the ideals of virtual geography transcend the realities of physical geography?

These and other prompts were necessary to articulate guidance and the boundaries of what we wanted to study so that our research could be pointed and relevant to the application areas.

As a subset of choosing prompts, Phase Zero requires the planning team to put a tremendous effort into curating subject matter experts. We invite experts to create and share a video or audio recording on their views of the state of technology, culture, ethics, economics, best practices, or other trends over the next decade that set the stage for how a future threat might come to pass. These specialists are usually renowned in their field and are selected to provide views that may challenge groupthink or expose workshop participants to factors not customarily considered during a business or military strategy session. Selecting, inviting, and gathering the experts and workshop practitioners is also referred to as curation.

Curating subject experts and inviting the right participants is one of the most critical components of the entire threatcasting method. These individuals generate ALL of the data used to do our analysis and report on the workshop's topic during the synthesis phase. In a later stage of analysis, we often consult external sources to fact-check our findings. Still, it is crucial that we honestly report findings based on the data generated by participants and the subject experts. Doing so reflects a specific (and arguably not a random) pool of expertise, biases, and diversification that we purposefully

build to avoid groupthink, bring in diverse or creative viewpoints, and estimate what practitioners might need to know so that we can find novel insights to future problems.

We choose specific expertise, diversities, and viewpoints because this reflects a comprehensive (and very early) assessment of *how* threats might appear. It also is an initial assessment of *who* might be needed to do something about these threats. Understanding the *how* and the *who* of this response to threats is an indispensable step in creating plans to avoid, mitigate, and recover from them. Filtering these inputs to the process is rightly subjective but in no way diminishes the quality of data generated in the following steps. The diversity of participants and the fact that we all bring our own biases and world views to the activity reflects the "human-centric process" of threatcasting (Vanatta & Johnson, 2019, p. 81).

The entire process of inviting the right participants and subject matter experts is at the core of a foresight technique called the Delphi Method (Helmer, 1967; Linstone & Turoff, 1975, 2011). Rowe and Wright (1999) suggest a traditional Delphi analysis needs to contain four features: anonymity, iteration, controlled feedback, and "the statistical aggregation of group response" (p. 354). Threatcasting uses Delphi differently than other foresight methods and emphasizes iteration and controlled feedback over the concept of experts anonymously and separately deciding on a range of actions. "To gather input from a broad range of global experts, threatcasting draws from the Delphi method, not only to capture the research and world view of experts but also to gather contradictory opinions and perspectives on the future" (Vanatta & Johnson, 2019, p. 80). Delphi traditionally seeks a consensus perspective from experts, whereas threatcasting welcomes (but does not necessarily seek out) contradictory opinions and diverse ways of seeing the

threat. Although threatcasting emphasizes scenarios that are stories of a person experiencing a local threat, often the resources needed to prepare for, mitigate, disrupt, or recover from a threat require people and processes across the globe. People in many places may be experiencing the same threat similarly, so we also seek perspectives that reflect geographic diversity when possible.

Another subtle difference in threatcasting's use of the Delphi method is purposefully avoiding subject matter collaboration. The subject matter experts who produce videos or audio recordings of their thoughts about the state of the future do not collaborate as they would in a traditional Delphi forum. However, the workshop participants interact and create shared stories imagining what the threat might look like in the future. The analyst is the person who aggregates the group responses after a workshop and becomes the point where the Delphi method loops back on itself and achieves consensus. These modifications of the Delphi method ensure that diverse (and often contradictory) perspectives are available during a workshop and afterward when the analysts consult participants again during the report evaluation phase. I discuss more how the Delphi method reappears during Phase Four.

Phase One: Research Synthesis

In Phase One, threatcasting synthesizes these contradictory perspectives by first drawing on the Delphi method of expert interrogation (Helmer, 1967). On the first day of a threatcasting workshop, expert interrogation begins with all workshop participants listening to subject matter expert presentations. Again, these experts share their thoughts

and assessments on the next decade of technology change, culture, ethics, economics, best practices, or other trends.

Following presentations from these subject experts, participants are divided into small groups to discuss the research and topics they just witnessed and begin to discuss whether any more significant implications are positive or negative and what the broad "we" should do about it. In the first feedback session, each group captures essential insights in a research synthesis workbook that is later fused with the larger group (Vanatta & Johnson, 2019). The research synthesis workbook becomes the starting point for random variables used to shape the raw materials of a probable future (albeit a fictional one). To choose these random variables, participants first capture the data points in the research synthesis workbook, list them one through *n*, and then use a randomizer - usually a dice with enough sides to cover each data point – to select about three of these variables. Participants then create a detailed story or scenario in the futurecasting phase.

The randomness of selecting data points ensures that each group begins their futurecast modeling event from a slightly different starting point. Coupled with the diversity of participants, their experiences, and their worldviews, usually ensures a much broader swath of possible futures is considered, modeled, and developed for further analysis. Too much similarity in models makes our understanding of the future threat myopic and more prone to missing critical knowledge about how the future could unfold.

Phase Two: Futurecasting

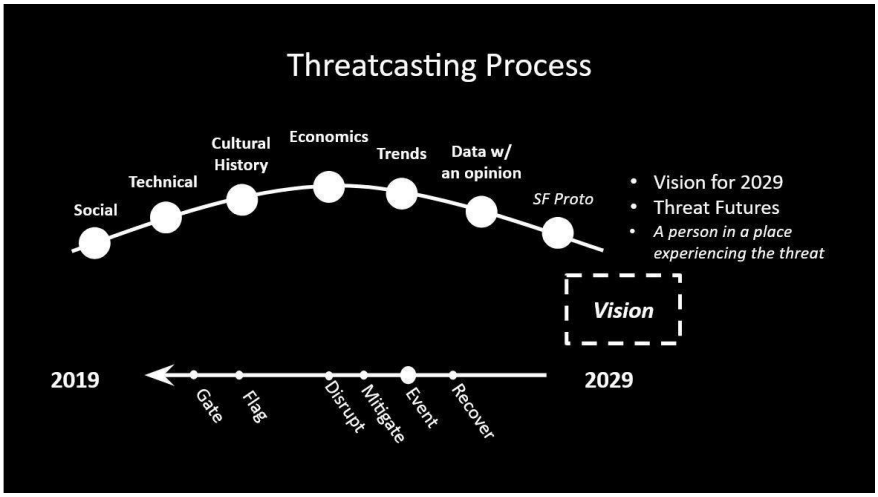
In Phase Two, we begin futurecasting or creating an effects-based model (EBM) that is similar to a science fiction future with "a person in a place with a set of problems"

set about ten years in the future (Vanatta & Johnson, 2019, p. 82). These models only describe the effects an organization wishes to achieve over the next decade. With a change in inputs, an organization can also model negative futures it wishes to avoid (Bennett & Johnson, 2016). Figure 3 graphically depicts Phase Two and Phase Three of threatcasting as a series of forward- and backward-pointing arrows meant to indicate futurecasting and backcasting, respectively. The combination of experience, design, and effects-focused modeling creates scenarios that illustrate with visceral detail the environment, the feelings, and the actions of a person, in a place, experiencing our threat problem. Again, understanding a fictional scenario in terms of desired effects reflects threatcasting's focus on the practitioner and how the findings will be applied.

Johnson & Vanatta (2018) postulate that forecasting beyond ten years begins to blur the plausibility of describing what a future may look like. Looking less than ten years out may not provide sufficient time to act upon the precursor events needed for that future to come to pass (Johnson & Vanatta, 2018). This is why threatcasting attempts to set a decade-long horizon in which to consider how a threat manifests. During a workshop, each small group generates a fictional prototype that follows a randomly selected ruleset from the synthesized data points from Phase One. Futurecasting means writing a short narrative that includes details of the person's story and life, including their name and other personal information, elements of their family & work, the environment that includes something about the nature of the threat, and their uncertainty about the future. At the end of the work session, each group will have identified a possible future threat and what effects that threat may have (Vanatta & Johnson, 2019).

Figure 3

Threatcasting Process



Note. The Threatcasting Process from Vanatta & Johnson (2019). Used with permission. Phase One includes the first five bubbles on the top arc; Phase Two is the last two bubbles leading to the "Vision" box on the right; Phase Three is the backcast depicted by the bottom arrow. Phase Zero and Phase Four are not on this diagram.

Phase Three: Backcasting

After developing the details of the threat and describing its effects on our model's protagonist, participants move into Phase Three. The goal of Phase Three is for participants to reverse engineer and map out the events that created their particular envisioned future. This "backcast" step uses a "time-phased, alternative-action definition (TAD)" process to work backward from the perceived future to "identify what could be done to disrupt, mitigate, and/or recover from their defined threat" (Vanatta & Johnson, 2019, p. 83-84). In the TAD process, "gates" are actions that defenders such as teachers, policymakers, industry, military, researchers, and others can control that help disrupt,

mitigate, or recover from a threat. To be very specific, the actual gatekeepers are the clients of the threatcasting project. We expect that the clients are interested in particular actions their organization needs to take to avoid, mitigate, or recover from the envisioned threat. In this phase, participants often identify other gatekeepers tied explicitly to specific gates, allowing the client to see how other actors may become engaged to help find solutions to the threat problem.

During backcasting, participants also identify explicit “flags” that should appear and often the order they are most likely to manifest. Flags are events within the environment (e.g., economic, geopolitical, cultural) or technological advances that defenders have no control over but influence the threat's development. By thinking through the chain of possible gates and flags along the timeline from the future to the present allows participants to consider the side effects of making disruptive changes to the timeline. Phases Two and Three are repeated between three and four times per group with different random inputs each time, again selected by a dice roll from the table of inputs recorded in the synthesis workbook. This allows participants to develop stories and scenarios with a broader range of possible future threats.

Phase Four: Post-Analysis and Reporting

Finally, in Phase Four, analysts take the workbooks and models as inputs to a separate post-analysis synthesis session. It is called post-analysis to distinguish from “pre-analysis” or the investigative work done in Phase Zero to establish the threatcasting foundation, research boundaries, and application areas. Post-analysis also differs from

Phase One synthesis, or the "in-stride" analysis that workshop participants do on all the inputs the subject matter expert panel delivers via video or audio recording.

In post-analysis, the moderators and members of the Threatcasting Lab use "multiple clustering and aggregation exercises to determine the patterns in all the futures modeled during the event" (Vanatta & Johnson, 2019, p. 85). I introduced these exercises in Chapter Two and will continue to illustrate how they appear during specific use cases in Chapters Four and Five.

As the analyst iteratively filters the data using various clustering and combination techniques, they should discover distinct patterns that describe how and under what conditions a threat should appear. These patterns are compiled into a final technical report, and some of the narratives of those patterns may be turned into a final, creative format. Previous threatcasting workshops have developed science fiction short stories, graphic novels, videos, or journal articles. The context and topics of the scenarios developed will help shape the stylistic choices of the technical report and any models chosen for development into a different medium. The outcomes from the threatcasting workshop are published in a format that speaks to various audiences, including the client, other gatekeepers, and those that workshop participants identified as critical to reaching (or avoiding) specific future scenarios. Data and analyses usually are made available through public access websites such as ASU's Threatcasting Lab unless the material is proprietary business information. How clustering, aggregation, theming, and other such "sausage-making" activities help produce insights and reportable findings will be the bulk of the remainder of my research.

A description of the sausage-making that occurs during post-analysis is non-existent in academic literature. Professor Johnson describes it like this:

> "There is a funny story here. For years I would never show my clients how the sausage is made - and they never cared. Once in a while, people would want to see it, and much like when people see how sausage is made - they would look away quickly. It was only when I came to academia that anyone actually cared at all to look." (B. D. Johnson, personal communication, February 6, 2021).

The opportunity to see under the hood and work with different futurists trained in threatcasting processes has given me an experience that most involved with threatcasting do not get to have. The majority of participants only experience threatcasting from the scenario development level. They develop their models at a workshop and return home. The next they will hear about the project is during a participant review after the analysis team has drafted the findings. Seeing the inner workings of the post-analysis process has been a valuable experience for me, and others need to know how to turn raw data into an analyzed product. It is here that investigating the processes and techniques in this phase is vital for linking the unique ways of doing things in the Threatcasting Lab with the richness of qualitative analysis methods from other fields.

Professor Johnson developed post-analysis as a three-round exercise (Johnson, Vanatta, et al., 2021). Each round has analytical goals to achieve before moving on to the next one, but returning to previous rounds is always necessary to ensure an iterative and complete process. Round one, named "Summarizing," prepares the raw data for analysis by confirming that each scenario summary contains all the bits of information that participants recorded during the workshop and that data are cleaned, anonymized, and checked for quality problems. When using a qualitative data software program, the analyst should also ensure that each scenario is correctly imported without errors.

Round two, or “Finding Meaning,” seeks to identify patterns and clusters within the raw data (Johnson, Vanatta, et al., 2021). The exact nature of how a new analyst should train their eyes and mind to recognize patterns is missing from threatcasting literature and is one of the primary gaps this dissertation seeks to fill. This is also the step the analyst will consider what information is missing from the effects-based models, thereby indicating where additional data may need to be gathered during report writing and the rounds of peer review that happen after post-analysis. This is also the round in which the analyst begins applying personal interpretation to develop patterns and themes across the models.

Round three is what Johnson calls “Finding Novelty” and seeks to identify the deeper patterns within the data (Johnson, Vanatta, et al., 2021). In this round, the analyst might ask: “How is the research question answered in a way that has not been addressed previously?” Or, “What information (patterns or clusters) might be useful to take specific actions in the application areas?”

In addition to understanding the whole process of threatcasting, analysts should be comfortable selecting the right analytical approach that best answers the study's purpose and the conditions under which they should or should not be used. A review of various theoretical frameworks might precede the decision to analyze in a particular way. In this project, I look at two: grounded theory development and a hypothesis-driven approach. There are also best practices and techniques from qualitative data studies that improve the analyst’s skills in coding, clustering, theming, note-taking, memoing, and so forth.

Seeking Novelty

I have referred to the idea of seeking novelty several times. It is both the name of the third round of analysis and a concept that is bigger than just a category of analysis. The step of recording novelty in round three is necessary to categorize and generalize the patterns in the data at as high a level as required to explain what is new about the future. There is also a subtly different understanding of finding novelty than I am seeking to uncover. This is the second gap of knowledge that this dissertation is attempting to fill.

I distinguish between the novelty found in round three of post-analysis and the emergence of extra-special implications of unprecedented futures that decision-makers are not prepared to address. I call the leap from novelty analysis to the critically important and distinctive understanding of the future "evolutionary novelty." This idea draws from the meanings of evolution in biological and psychological sciences and implies irreversible adaptations to respond to environmental and sociological threats. For threatcasting, an evolutionary novelty illustrates the rare or anomalous finding that fundamentally shifts how we perceive the impacts and effects a threat creates in the future.

An example of an evolutionary novel finding can be found in *Information Warfare and the Future of Conflict: A Threatcasting Lab Report* (Johnson et al., 2020). Researchers on this project found that the character of conflict in the future is no longer binary, meaning we can no longer divide the idea of conflict into the state of being at war or the state of being at peace. Instead, due to the far-reaching and ubiquitous access to automation, social media, a 24-hour news cycle, and plenty of leaks of personal

information, we should "adopt Quantum [sic] state approaches where the nation can be both at war and at peace at the same time" (Johnson et al., 2020, p. 11). This challenges, or critiques, the long-standing approach to conflict because our national security and defense strategy thinkers continue to view conflict as binary. The evidence from the threatcasting process is that it is *not* either at war or peace. This declaration is an irreversible adaptation to our understanding of conflict, given the current and projected state of technology, politics, and society. Therefore, it is an appropriate example of evolutionary novelty.

In summary, this chapter provided a step-wise overview of the four phases of threatcasting currently extant in the literature. It introduced the terms and concepts needed to begin a deeper interrogation of threatcasting post-analysis. This chapter also raised the importance of Phase Zero planning and research and proposed a new term, evolutionary novelty, as a concept for more advanced post-analysis practices. In the following two chapters, I will investigate the strengths and weaknesses of two different approaches to post-analysis - the grounded theory approach and the hypothesis-driven approach - and use them to demonstrate part of my personal growth as a researcher and futurist. I will return to the distinction between novelty analysis and evolutionary novelty again in Chapter 6 but needed to introduce it here first to establish a common language for the rest of this study.

CHAPTER 4

CASE STUDY: THE FUTURE OF WMD

Introduction and Inductive Analysis

This chapter introduces the first of two approaches to analyzing raw data from a threatcasting workshop. This approach uses an inductive methodology to seek findings and conclusions using the three-round post-analysis approach developed by Johnson: 1) summarizing, 2) finding meaning, and 3) finding novelty (Johnson, Vanatta, et al., 2021). The analyst uses an inductive perspective to discover appealing details and findings from within the data itself. There is no preconceived framework or set of points to confirm, deny, support, or refute. The analyst lets the data themselves guide what is notable and how conclusions should emerge. However, it is the data and the analyst together that bring about conclusions and findings. Each analyst has a perspective on life, worldviews, and even biases that must be accounted for and appreciated. This is why the threatcasting methodology seeks diversity in its members; it's a design feature to use bias, background, and experience to develop and recommend actions that others can take to avoid, mitigate, or recover from future threats.

The inductive method is strongly associated with grounded theory approaches to qualitative data processing and analysis. Charmaz (2000) states that a grounded theory provides "a useful conceptual rendering and ordering of the data that explains the studied phenomenon. A grounded theory is durable because it accounts for variation; it is flexible because researchers can modify their emerging or established analyses as conditions

change or further data are gathered" (p. 511). What this means for threatcasting is that grounded theory and the rich academic literature using its techniques support threatcasting's messy approach to analysis. It is messy not because there is a lack of process but because each project is uniquely striving to answer difficult questions about the future that are not amenable to objective or quantitative calculations. The future is inherently unpredictable, yet the processes of threatcasting give us just enough structure to make a little bit of sense of what could happen if the right conditions appear.

A grounded theory or inductive approach's strength is that descriptions of the findings can come from within the data. *In vivo* coding techniques are used to describe something the data tries to say in the words of those trying to say it. Analysts use the words of the model or raw data to describe the effects that they are trying to model. Process coding looks for action in the data and labels those with gerunds ("-ing" words). In contrast, concept coding techniques "lump" together ideas into more abstract or more generalizable contexts threaded between several models (Saldaña, 2016). Each of these coding and clustering techniques depends on the data telling a story to the analyst and the analyst interpreting how the story is "grounded" in a description of how the world could turn out.

Pre-Workshop Activities

To demonstrate how the inductive approach is the core technique for post-analysis, I scrutinize post-analysis processes deeper than other publications on threatcasting. A case study investigating the future of weapons of mass destruction (WMD) and cyber effects in the year 2030 demonstrates the fundamentals of inductive

analysis. It is necessary to set the baseline for other projects before investigating approaches in which grounded theory or induction methods are not entirely sufficient or fall short. This project was a collaboration with the Army Cyber Institute at West Point (ACI) and the Defense Threat Reduction Agency (DTRA) to respond to imagined threats at the nexus of WMD and cyber technologies. The threatcasting foundation, which includes the narrowed topic, the research question, and the anticipated application of the project's results, set the project's boundaries and output goals (see Table 1).

Table 1

The Threatcasting Foundation to Study the Future of Cyber & WMD

Topic	The future nexus of WMD and cyber threats in the year 2030
Research Question(s)	What is the threat landscape for cyber coupled with WMD threats? How are these threats identified, characterized, and categorized?
Application Areas	• Identify "Centers of Gravity" which can lead to cascading WMD level events; • Collate/map categories of threats in terms of Payoff, Difficulty, and Ease of Attribution; • Characterize differences in impact from traditional WMD vs. non-traditional (WMD + Cyber) threats; • Determine if the definition of WMD should be expanded beyond CBRNE; • Identify mitigating actions DTRA should take; • Identify with whom DTRA should partner.

Note. A threatcasting foundation contains a well-defined topic, research questions to guide the data collection, and application areas that recommend actions gatekeepers may take.

As I started working on the WMD and cyber project, it appeared that it would be a straightforward event aimed at providing our government clients a few answers about what they should consider about cyber and WMD threats over the next decade. But because Professor Johnson asked me to take a more significant role in the preparation stages and the post-analysis phase, I recognized this was an opportunity to make detailed observations on the inner workings of Phase Zero and Phase Four activities in which I was not previously involved.

I first recognized that I needed to expand on a few gaps in information that were not listed in the overview of the threatcasting methodology in Chapter 3 but were critical to this project's success. Primary among these gaps is a more detailed description of what happens during Phase Zero, including developing a steering committee, inviting participants, conducting preliminary research, and seeking subject matter experts to fill in our knowledge gaps.

We started by creating a steering committee from representatives from ACI and DTRA. They helped solidify the threatcasting foundation, including the project's scope, relevant research questions, and application areas for the results. The project’s scope was partly defined by the federal government’s call for papers on innovative ways to facilitate discussions on WMD, cyber, and deterrence issues (United States Air Force Academy, 2016). The committee interpreted this call for information to mean that threatcasting methodologies could be uniquely leveraged to find creative ways to open the dialogue on the future of WMD and cyber attacks.

The steering committee included individuals working within ACI or DTRA who had access to the current “feel” of the state of affairs in the world of cyber weapons and

weapons of mass destruction. They also had access to experts within their respective fields either within the organization or through contacts in academia, industry, government, or elsewhere. Using their personal and professional contacts, the steering committee nominated subject matter experts and participants who would best help us achieve the threatcasting foundation requirements. The credibility of the steering committee members strengthened the importance of the project for nominating and then choosing the right people who were best suited (and available) to answer the threatcasting foundation.

As part of the government's call for papers, the steering committee assessed a need to include research on the topics of biological, nuclear, chemical, radiological, and explosive weapons as well as cyber experts from both the offensive and defensive sides of that mission (United States Air Force Academy, 2016) and nominated experts from each of these topics. We collected unclassified research and white papers on nuclear proliferation, weapons monitoring, and previous government assessments of WMD programs to get a baseline understanding of the state of the world in these areas and some anticipated trends. We also looked for subject experts that would augment our grasp of technology trends and political factors in the development and proliferation of cyber weapons and the various types of WMDs. Some of the initial subject expert nominees included a few well-known scientists, engineers, technologists, authors, entrepreneurs, and some not-as-famous but still highly respected academics, industry leaders, and government employees.

Although these subject expert recommendations began quite broadly, the committee whittled this down to a more manageable list over several weeks, primarily

due to access and availability after sending out initial invitations. Once the steering committee narrowed the list of experts to a reasonable and approachable list, members of the Threatcasting Lab interviewed the individual SMEs. They recorded a brief video explaining their thoughts on the future of WMD and cyber in the year 2030. In total, we recorded ten videos from experts on the topics of bioterrorism, weaponization of synthetic biology, nuclear technologies, and other pertinent areas to create a core of knowledge for workshop participants and analysts. These videos were then used as inputs to Phase One of the threatcasting workshop.

Simultaneously with nominations for subject matter experts, the committee suggested a list of people who would be valuable participants for the intensive two-day workshop held at the ASU campus in Tempe in February 2020. These participants included practitioners from industry and government, researchers from academic institutions and think tanks, researchers from industry R&D programs, as well as law enforcement and emergency response units from several metropolitan areas. In total, over 60 people responded to our invitation to participate in person. Participants were then assigned to teams of 3-4 to begin futurecasting and modeling.

Additionally, staff from the ASU Threatcasting Lab and ASURE, a partner ASU organization, organized the conference room and amenities to host over 60 people and keep them caffeinated and fed for the duration of the work session. The selection, invitation, and gathering of SME inputs and work session participants concluded Phase Zero of the threatcasting process.

The Workshop: Creating our Models

During the workshop, Brian David Johnson, Threatcasting Lab Director, and Natalie Vanatta, senior advisor to the Threatcasting Lab, facilitated training on how the threatcasting process would run and then assisted the development of effects-based models as described in Chapter 3. Overall, teams developed 44 models to imagine how in the future, weapons of mass destruction and cyber threats would interact in the year 2030. The models and the findings of this workshop are in the final report (Johnson, Brown, et al., 2021).

What is not in this final report is a discussion of the "sausage-making" that the analytical team needed to go through to reach the conclusions and findings that eventually resulted in the final report. This analytical process is the purpose of the remainder of this chapter.

To begin, I need to set the stage for how external factors and the political environment influenced the analysis. First, as a reminder, the data modeling work session was held in February 2020, right at the beginning of the worldwide recognition that increased cases of pneumonia from unknown causes were beginning to spread outside of China (World Health Organization, 2020). News reports worldwide speculated on the source, lethality, and potential spread of what later was to be labeled as the COVID-19 virus. Governments had not yet begun implementing action plans to quarantine and curtail the spread of a potential pandemic vector, but I am confident that many governments were starting to prepare their plans.

It is essential to include this context of an emerging global awareness of a biological threat as it clearly impacted workshop participants' thinking. During the first round of modeling held in the afternoon of the first day, most of the 15 groups developed models based on biological vectors, often coming from a threat actor who had used readily available genetic manipulation techniques to create tailor-made viruses and bacteria. Eleven of the models suggested that these tailor-made biological threats could be genetically targeted at specific populations or could be spread in a way that avoids current medical detection today.

When the workshop moderation team recognized the similarities of many of these models, they asked participants to include other aspects of the WMD-cyber nexus in the second round. Fifteen more models were created, and the threats opened up to incorporate radiological, nuclear, and explosive hazards. During the third and final round of modeling, participants were asked to focus on cyber threats with a sprinkling of WMD components rather than the other way around. We ended up with another fourteen from this perspective, bringing the total to 44 unique threat futures.

At first, it may seem that asking teams to narrow in on smaller slices of the range of possible and probable threats would limit the creativity of those imagining future threats and scenarios and may induce additional bias. However, this is not the case for two reasons. First, recall that the purpose of creating models of the future is to answer the needs of the threatcasting foundation. In this project, the models need to answer the research question, “What is the threat landscape for cyber coupled with WMD threats?” Because of the influence of the emerging event that would later become the COVID-19 pandemic, the facilitators knew from the first round that they could not answer the

research question without additional data from threats other than biological and genetically modified viruses.

The second reason that a narrow focus was warranted was that it allowed the models to answer the foundation's application areas. This will enable practitioners and decision-makers to receive focused and relevant recommendations for solutions to emerging or potential threat futures. Reducing the irrelevancy of creative and far-flung futures undoubtedly limits the field of what is *possible*, but it also narrows the focus to what is more likely and more *probable*. This produces a much more manageable set of scenarios that can be weighted and prioritized for allocating limited resources such as those needed to detect the flags and gates of a threat emerging or for implementing solutions to mitigate, disrupt, or recover from a threat.

In short, we needed to steer participants' thinking away from the short-term threat of the developing COVID pandemic and towards other equally probable threats in the next decade. This illustrates why moderating inputs between rounds of modeling is both necessary and allowable and is encouraged in the threatcasting framework.

Post-Workshop Analysis

Professor Johnson led the analysis of the data generated by the workshop held in February 2020. Johnson requested that Josh Massad and I, acting as supporting analysts, follow the typical data analysis approach as outlined in Chapter 3. The three-phase post-analysis moves through the data by summarizing, finding meaning, and finding novelty. This standard approach assumes no conclusions at first and reflects the spirit of grounded theory analysis.

Despite each analyst following the three-phase inductive process, we used our own way to find meaning and find novelty. By this, I mean that there was no external framework we were trying to prove or disprove other than seek to answer the threatcasting fundamentals. Johnson prefers to record his coding and summarize directly in Excel or Google Sheets workbooks, using different columns to track each phase. In contrast, I prefer to use qualitative analysis software and then later export my analysis to fit into Johnson's format. I conducted my analysis starting with a series of multiple passes through the data. The first focused on processes by identifying "-ing" action words such as: "trusting machines to tell us the (wrong) truth," "misunderstanding killers," and "exploiting disinformation during [an] event of mass effect." The second pass-through focused on structures within the models (e.g., flags, gates, milestones, and vulnerabilities in which I looked for commonalities between each of these structure types). The third pass-through focused on concepts, or words and short phrases that "symbolically represent a suggested meaning broader than a single item or action - a 'bigger picture' beyond the tangible and apparent" (Saldaña, 2016, p. 119). Concept codes in this project included ideas such as "cyber as a disrupting tactic," "genomic data is an untapped criminal enterprise," or "ransomware as a service." These codes were later collected into broader categories and themes.

Figure 4 is an excerpt from our combined post-analysis workbook and shows five columns. The sixth column ("Round Three - Novelty) will be discussed more in-depth in Chapter 6. Column A is the round in which the group created the model. Occasionally, round one lacks some detail in the model since members of each group are just getting to know each other and are still trying to figure out the process of futurecasting and

backcasting. It helps the analyst see what ideas a team latched onto in each round, how the team matured together throughout the process, and how previous ideas transitioned into new ideas between models.

Figure 4

Standard Post-Analysis Workbook

Round	Team	Round One - "Summary"	First-pass coding	Round Two - "Meaning" / "Insight"
1	Yellow Pawn	A woman in the developing world. Her name is Rashida. She looks like a Disney princess. Other scientists in the lab, and a large tight-knit family.She lives in Isfahan , Iran, where she works as as a pathologist.She is investigating samples from various patients to ascertain if Crimean Congo Haemorraghic Fever is zoonotic and potentially linked to breeds of livestock that are critical to their way of life.She experiences the threat through both researching the issue and being a food consumer in the community. Second/third order effects in community blowback from operators of the food chain, rumors of the threat being engineered, lack of trust in food sources, increased food insecurity in the community/country.Colleagues, family in Isfahan, farmers, butchers, local government, maybe the state government. The Adversary seeks to promote instability in Iran and ultimately undermine the regime. Promote mistrust in Iran's central government; concerns about the food supply, with associated chaos; suspicion concerning scientific research and innovation and the risks posed. (Vulnerabilities) Mistrust of the goverment, vulnerabilities in the food supply, level of science literacy.New diseases in Iran, links to an actor placing the new disease there to affect the food supply. Accusations and mistrust between governments. Local panic and riots. New genetic sequences are found in the new disease, makes it look suspiciously like it's been engineered, rather than naturally occurring. (Barriers) Biological Convention bans the uses. Scientest that would be needed to make it would have ethical issues. Politically, who calls for this attack will need to be Confident that they will get away it/not get caught. (Rsx pipe) The ability to change/modify/create viruses is already avaliable today. Will continue to be refined in the future. (G) Biological Weapons Convention. (G) Widened, random testing for/surveillance of threats within food chains. (G) Inspections at borders to identify, confront, and/or disrupt threats. (F) Access to/knowledge of what all nation-states may be doing in the space. (F) Access to/knowledge of what individual actors may be doing in the space. (M4) Better surveillance/test protocols. (M4) Confidence-building measures to promote trust among stakeholders: countries, governments, communities. (M8) Legislation WIth defined punishments to help deter any future attack - eg economic sanctions against states found to have developed or deployed zoonotic agents	Exploiting disinformation during event of mass disruption; Food security is a social & economic center of gravity; Mass disruption is more unpredictable than mass destruction; Bioengineered mistrust as tool of conflict; Private sector goods are still infrastructure	Tipping the chain of attack; Preparing for atrocities before they happen; It's always been about disruption; Biology is programmable; Detection is necessary to develop good responses
1	Grey Pawn	Nakita - affluent black female nobel prize winner 30 under 30 entrepreneur Rich academic society; active in BLM and other activist orgs Nutley, New Jersey; entrepreneur in genomic engineering Trust in data down the stream; trusting in her coworkers As a black female, she is victim to mass panic and race-related flash mobsHer family members and community via mass violence enticed by studies based on manipulated dataCoworker: monopolizing medical solution via manipulation of public data base; Researcher: publishing a popular paper; Alt Right groups: enticing violence to satisfy race related agenda. (Vulnerabilities) Lack of integrity/security in open public database; fueling stresses in identity politicsSource effecting will effect all downstream uses including acadamia and errode confidence A basic science effort has immense consequences to society. (Barriers) Becuase of the nature of open source databases, there are very few barriers to data manipulation. (Rsx pipe) Machine learning could be used to make manipulation virtually undetectable. (G) Measures in place to ensure integrity open source data. (G) Multiple agencies for checks and balances of data (control group). (G) Publish or die minimizes integrity check. (G) Media sensationalization. (F) Monopoly on dataset. (F) Growth of unchecked fake news for the sake of sensationalization. (M4) Integrity standards on shared genomic datasets. (M8) Chain of custody for input integrity. (M8) Immense growth of dataset; making manipulation impossible/impractical	False info incites fear, panic, mobs; Manipulation of public databases; AL & ML to hide attribution; Speed to market is enemy of info integrity & security	A safe space is a secure space; Cyber as integrated computers in warfare; It's always been about "disruption"

Note. Excerpt of two scenarios from the raw data workbook after first and second pass coding is complete. The third column (Round One: "Summary") has the concatenated summary from the workbooks.

Column B is the team's name. These names come from a colored game board piece that each participant receives when they arrive at an in-person workshop. Team members must find their team by seeking out those with the same color game piece. Creating innocuous team names such as "Yellow Pawn" or "Blue Chip" avoids the awkwardness of coming up with team names or attributing personal information to a process that should not be influenced by the strength of personality.

Column C is the “Round One - Summary.” There are two ways to get this summary. The first way, and the one displayed in Figure 4, is simply copying and pasting the answers given to each of the prompts in the session workbooks into a single paragraph. I usually insert short keywords breaking up the sections of this paragraph to indicate where transitions occur from the workbook. For instance, the WMD workshop models had questions that transitioned between vulnerabilities, barriers, and other parts of the research pipeline, so I inserted a parenthesis with those keywords before that section. This allows me to scan for those transitions within the summary paragraph quickly.

The second way to do the summary section is to copy and paste the same answers to a singular paragraph and then rewrite the summary as a simplified scenario that captures the key points, usually in a chronological or other logical order but doesn’t strip away the details. As many of the original sentences and phrases that participants wrote would remain as possible. This prevents distorting the richness of *in vivo* concepts that might capture the idea better in the original than from a re-telling. The benefit of this simplified summary is to clarify the intent and narrative of the model, especially if the participants recorded bullet points or truncated ideas. Since the participant workbooks are set up as question-answer prompts, many groups simply answer the question assuming the context is evident because of the prompt right next to it. Copying just the answers to these questions into a block paragraph strips away the context and requires the analyst to refer back to the prompt to understand the short phrase or bullet point.

Column D is a place to record the first passes of coding. As I described in chapter 3, I prefer to take several looks at the data in the first pass, each time looking for different types of codes. Marking the summary with structural codes (e.g., gates, flags, milestones,

and vulnerabilities) allows me to filter all excerpts with the same codes and quickly see any commonalities between each structure category. This gives a deeper understanding of what we can recommend gatekeepers should do in the application areas of our threatcasting foundation. This column is a new addition to the spreadsheet Johnson has been using, and it is one I have encouraged him to adopt in future projects. Recording ideas from the first pass of coding is crucial because it allows all the project analysts to see the language, keywords, and codes that other analysts find from within the data. This improves inter-rater reliability for subsequent rounds of analysis and across the remainder of the models.

Column E, labeled "Round Two - Meaning / Insight," is where we record our ideas on the clusters and categories of codes that begin to form during the first pass of coding. I often consult my memos as they help me recall how I phrased categories, as the connection between ideas sometimes comes "in the moment." Without memos, I struggle to recall these "moments" of inspiration. The "meaning" or "insight" that this column represents is just one step away from a reportable finding. In other words, the category of "it's always been about disruption" encapsulates child codes such as "cyber as a disrupting tactic," "scaring as a tactic," or "compromising the supply chain of synbio industry programs." Each of these child categories appeared only once or twice in the first round, and I decided that the idea of "disruption" was a better category that described them all.

One technique that Professor Johnson used in this analysis was to send me a transcript of his thinking aloud. As soon as Johnson completed his analysis of "Round Two - Meaning / Insight," he recorded himself using the Google Docs voice-to-text

feature as if he were talking with a colleague. This “think aloud” session tied the categories' names to the codes and clusters. Then he provided some justification for his ideas from both the raw data models and his observations.

> “Okay, so first, the category is ‘a safe space is a secure space.’ I described this one as a system that could be cyber-biological-nuclear, etcetera, that has security as a core feature, and oftentimes this is designed with a failsafe mode already built-in. The code is also used both for the security of the system as well as the idea of safety so that [includes] physical safety or social safety. Another concept within this category is having a physical fail-safe that is an analog to digital technology. Another idea is the venture capitals’ push-to-market mentality that leaves security on the back burner sometimes. This also encompasses ideas of personnel reliability and checking up on the security of people within our systems.” (B. D. Johnson, personal communication, March 24, 2020).

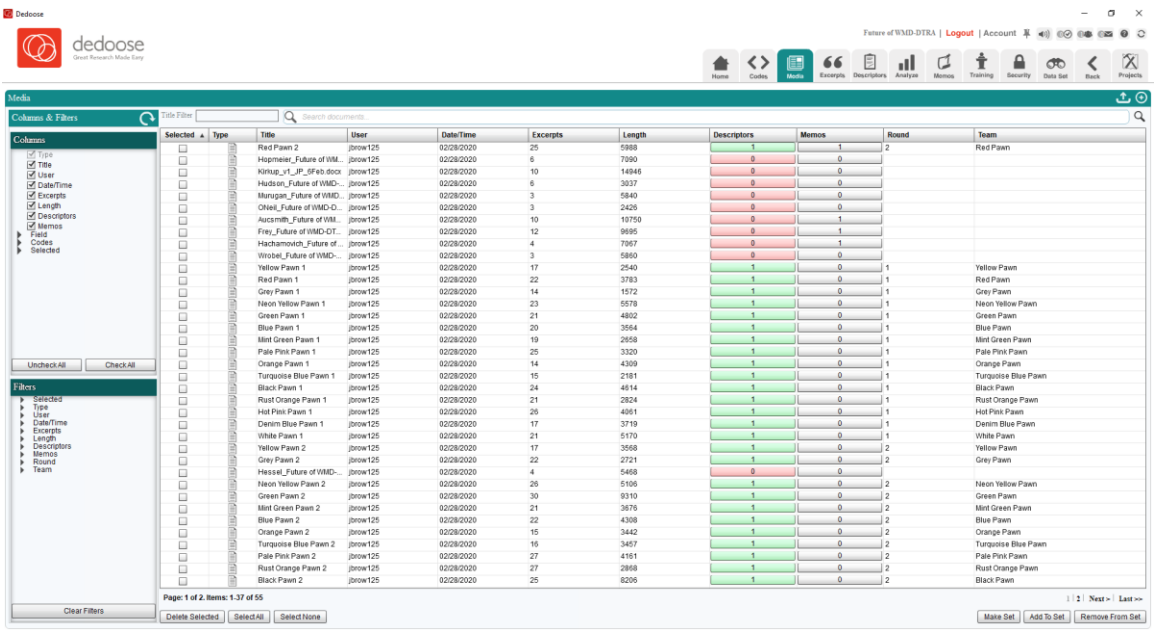
A Google Sheet or a Microsoft Excel file is not the only way to record codes, clusters, and categories. Rather, these tools are probably the most useful for collaborating with team members across multiple states and time zones and provide a historical record of the analytical team's decisions in a familiar format for reference at a future date. Many brands of qualitative analysis software are available to the researcher. I used the Dedoose platform (SocioCultural Research Consultants, 2020) to track codes and combine codes into clusters and themes. Using Dedoose allowed me to rapidly include or exclude data excerpts with various codes to investigate emerging ideas and test how they made sense.

Dedoose is a type of CAQDAS (computer-assisted qualitative data analysis software); of the many programs available, this was the one that offered me the functionality best suited for my purposes. There are some drawbacks to using any CAQDAS, including the learning curve to understand the buttons and interface and the difficulty of getting semi-automated data analysis capabilities to work consistently. The analyst still needs to interpret the charts, graphs, and other analytical aids that software

produces. Software-based analysis is a tool and not a panacea; the analyst needs to understand when to use its outputs and when to use other tools or methods to verify and collaborate findings.

Figure 5

Dedoose Screenshot of the Media View Page



Note. This screenshot shows the media view within Dedoose. Each line is a single scenario or one of the transcripts from our subject matter experts.

Another strength of using Dedoose is the ability to link analyst memos to different tags, codes, and excerpts from the data. Analyst memos help keep track of ideas that trigger off of previous ideas. They are used to justify and explain why the analyst decides on specific code labels. The analyst can also use memos to record conditions and external factors that influence the analyst into thinking about the data in various ways. This helps

identify sources of bias or gaps in the analyst's approach. Saldaña (2016) considers memoing an essential skill for the qualitative researcher. He says,

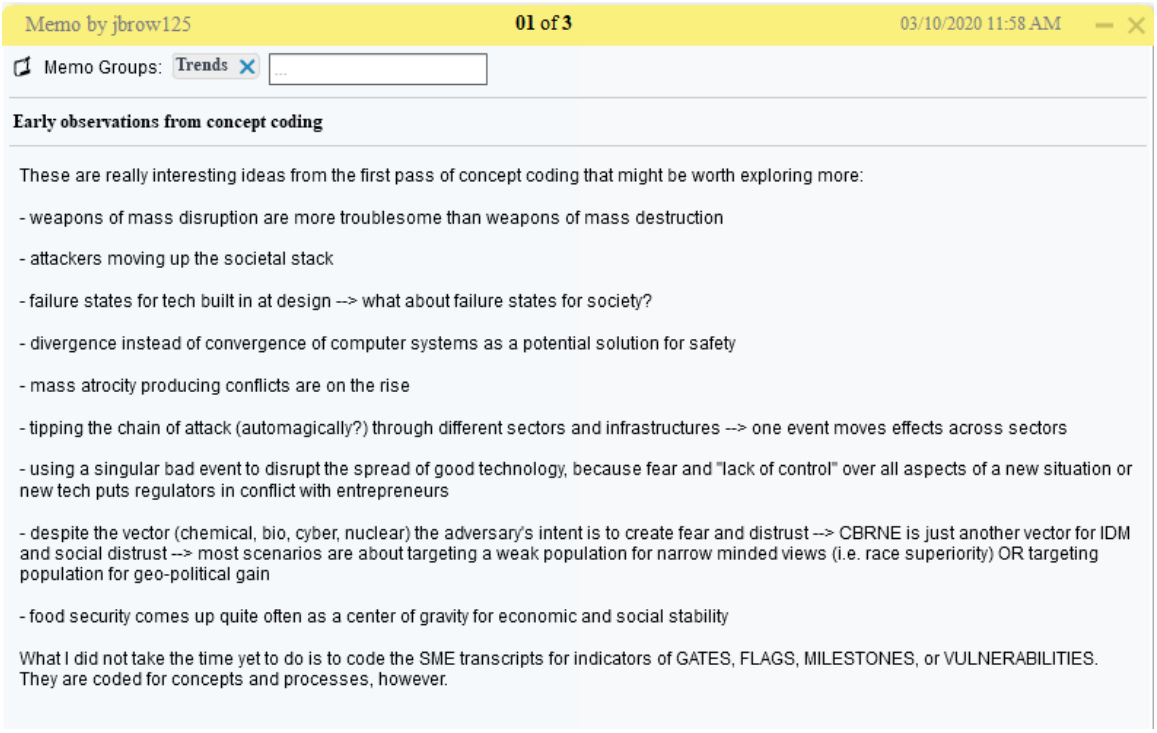
> "Think of a code not just as a significant word or phrase you applied to a datum, but as a prompt or trigger for written reflection on the deeper and complex meaning it evokes...The writing thus helps you work *toward* a solution, *away from* a problem, or a combination of both" (p. 44, emphasis in the original).

These memos help trace what I was thinking about and how codes began to connect. For example, in a memo dated 10 March 2020, I wrote about the idea of "tipping the chain of attack" (see Figure 6). I took this to mean that effects were initially observed or felt within one sector but continued to ripple into other sectors until a catastrophic scenario began to disrupt society and social systems. The first instance of this "tipping" started with the Pale Pink Pawn 1 scenario in which a vaccine intended for treating some type of disease in humans ends up contaminating fisheries and causing a genetic mutation in fish. Although the vaccine's protein structures were heavily modeled by quantum computing, side effects on other species were not modeled. The immunization subsequently decimated the fish population, causing a food shortage in Vietnam. The food shortage rippled into other aspects of social well-being, and the economy took a downturn.

The next instance of "tipping" appeared in the scenario by Yellow Pawn 1. This time the vector came from a hemorrhagic fever that materialized in Iranian cattle and was lethal to humans. This tipping, coupled with rumors that the fever was engineered and purposefully placed to target Iranian society's well-being, manifested again within the food chain and soon spread to other parts of societal order and safety.

Figure 6

Early Observations from Concept Coding



Note. This memo records my observations during an early round of concept coding and has early indicators of conclusions that I would eventually transfer to the "Finding Meaning" round.

Another instance of "tipping" that was not related (directly) to food security came from the Neon Yellow Pawn 2 model. This time, the city of Memphis had a cascading effect on social order and safety when residents received city-wide automated cell phone alerts, similar to an Amber alert, about a radiological device exploding within the city. Artificial intelligence programmed to control the radiological detection devices should have issued warnings and alerts based on the sensors. Unfortunately, the AI was not well-trained in how to spot a hacked system. Panicked people quickly flooded 911 and other

emergency response channels seeking information. When public communication circuits were overloaded, there was no one to validate the threat, and people began pillaging food, water, and other essentials. Roads exiting the city quickly became jammed with fleeing vehicles.

Finally, the concept of "tipping the chain of attack" was emphasized by the inputs several subject matter experts introduced in their videos. One idea suggested mass atrocities should be considered processes rather than events. Another discussed how cyber threat actors use social engineering as the initial point of entry into a computer system to attack critical data and move from one system to another. With the data from at least a dozen models, these ideas strongly suggested that a threat actor would not need to spend the time, energy, and money to disrupt government and national decision-making directly. Instead, supposing they released a small virus that could leap through the food chain, causing panic, confusion about the truth of information, and fear about food safety and stability, they could achieve their goal with ease.

It is essential for the analyst to understand and document their biases and remove, or at least account for, them if appropriate or to justify and acknowledge biases if it is central to the project. For the most part, allowing certain types of analyst bias to remain is a feature, not a flaw, of the threatcasting methodology. Acknowledging the strength of perspective from years of experience is necessary to better answer the threatcasting foundation and recommend action items to practitioners. In this sense, bias is not pejorative, and we should not automatically reject it as a source of error in the project.

Despite each of us analyzing data our way, we needed to also come up with a shared set of conclusions and produce a unified set of findings. Over the course of a few

meetings, Professor Johnson, who led the post-analysis, took inputs from Josh Massad and me. We discussed why I used terms like "tipping the chain of attack" (which eventually made it into the final report as such). Johnson chose to use "destabilization" as the central idea before settling on a framework of three categories: Cyber aided WMD, biological hybrid, and digital weapons of mass destabilization. One fascinating concept developed around destabilization and its effects on military operations and can be seen in the bottom-right cell in Figure 7 and is quoted here for clarity:

> "This category might be too broad; are there different forms of disruption? Is disruption a by-product of different types of threat actor goals? What about disruption by a naturally occurring mass event? WMD have always been weapons of mass destablizations [sic] in order to get other goals achieved (surrender, etc.) and adding the digital/cyber component to destabilization is a force multiplier."

Figure 7

Excerpt of Categories After Second Round of Coding

Number	Label (goal of 7 +/- 2 labels)	Description/Definition	Indicators or Flags	Examples	Next Steps
1	A safe space is a secure space	Designing a system (cyber, bio, nuclear, etc) with security as a core feature; often with fail-safe mode. This code is used for both the security of the system as well as for the idea of safety, whether that's physical or even social safety.	"monocultures of IoT devices"; physical fail-safes in tech-enabled transportation; Venture capital "push to market" mentality leaves security on the back burner; personnel reliability programs for Cesium replacement program;	Mint Green Pawn 3; Neon Yellow Pawn 3; Green Pawn 2; Orange Pawn 1; SME-Kirkup; SME-Aucsmith; SME-Hudson	
2	Biology is programmable	Programming or using biological tools for targeting groups, xenotypes, or individuals using CRISPR and DNA manipulation or designer drugs.	using stem cells to revert CRISPR modifications; organic & higher priced foods are safe from DNA manipulation; viruses targeting Hispanic xenotype	Hot Pink Pawn 3; Rust Orange Pawn 2; Black Pawn 1; SME-Kirkup; SME-Hessel	
3	Cyber as integrated computers in warfare	Hacking, manipulation of digital data, using AI for detection or hiding attribution, or the use of online & cryptocurrency transactions to hide attribution are techniques of the cyber enabled warfare. This also covers cyber attacks against cyber or cyber-physical systems.	Hacking of IoT devices or personal cell phones to suggest a targeted message; use of cryptocurrency by criminals/state actors to create plausible deniability; attacking cyber-physical systems and SCADA	Denim Blue Pawn 3; Mint Green Pawn 3; Green Pawn 3; Black Pawn 2; Neon Yellow Pawn 2; Grey Pawn 1; SME-Aucsmith	SCADA systems rely on older tech, and are not likely to be updated soon; connected computational devices --> digital components get you the "M" in WMD
4	Detection is necessary to develop good responses	Detection of materials, evidence of manipulation or criminal activity online, and filtering social media for indicators and warnings of a threat event or precursors to a threat. This also includes detection of medical pandemics or extremist ideology radicalization.	identification of social media chatter indicating an event has or will occur; conducting activity below the threshold of current detection capabilities; research on detection devices; evidence of unethical research on bulletin boards	White Pawn 2; Turquoise Blue Pawn 2; Red Pawn 1; Green Pawn 2; SME-Murugan; SME-Wrobel	The meaning behind this is threat actors understanding detection thresholds and maneuvering below that level --> many scenarios talked about increasing the detection threshold through policy & research but this doesn't exclude thinking about new things to detect!
5	It's always been about "disruption"	When social order shifts negatively from the norm, or when a sequence of events produces further damage and disruption to infrastructure, social order, or the economy. This may occur when a threat group purposefully introduces an event of mass effect or if a threat introduces a small event that leads to mass atrocities or social disruption.	political blame and political tensions increase; manipulation of trusted data and information (i.e. IDMs are used); compromise of supply chain; attacking the population for mass chaos and fear; local event triggers a chain that spreads geographically;	Denim Blue Pawn 3; Hot Pink Pawn 3; Orange Pawn 3; Pale Pink Pawn 2; Black Pawn 2; Neon Yellow Pawn 2; White Pawn 1; Rust Orange Pawn 1; SME-Frey; SME-Hachamovich; SME-Kirkup; SME-Aucsmith; SME-ONeil; SME-Hopmeier	This category might be too broad; are there different forms of disruption? Is disruption a by-product of different types of threat actor goals? What about disruption by a naturally occurring mass event? WMD have always been weapons of mass destabilizations in order to get other goals achieved (surrender, etc) and adding the digital/cyber component to destabilization is a force multiplier

Note. Excerpt of the categories developed after the second round of coding (finding meaning). The bottom right block is the first time we recorded the idea of "weapons of mass destabilization," which later became a central theme of our final report.

Eventually, the analytical team developed a consolidated codebook based on each analyst's inputs and a discussion about how to generalize best our observations of the themes or categories of ideas spanning the majority of the models. We tried to keep the final codebook between 5-7 entries, which provided enough variety to ensure concepts were not over-generalized. A larger codebook runs the risk that outliers, or those ideas that are seen only once or twice across all the models, will become inadequately weighted in our analysis. Unless an outlier is critical to understanding a threat that no one else was talking about or was so unique that it required additional attention, it often gets dropped in favor of more conspicuous ideas. There were no singular outliers that met this latter "uniqueness" criteria in our analysis, so a codebook of three items ended up being just about right (see Figure 8). Although code #1, "Cyber Aided WMD," was the more generalized category, we specifically allowed for codes #1a ("Before: Opportunity"), #1b ("During: Assistance"), #1c ("After: Amplify"), and #1d ("Ubiquitous: Falsify") to categorize the temporal aspect of cyber-attacks occurring in the same event as a WMD. We wanted to illustrate this finding because some gatekeeper actions were more influential in one or two phases of a cyber-aided attack and less appropriate to consider in other stages.

Figure 8

Final Codebook for the Project on WMD and Cyber

Code Number	Label (goal of 7 +/- 2 labels)	Description/Definition	Examples
1	*Cyber Aided WMD*	*Do not code with this category; use 1a-1d instead*	-
1a	Before: Opportunity	Use cyber tools/techniques to open a window to a vulnerability (i.e. "unlocks and opens the door")	Creating holes in security systems of portable nuclear generators to initiate an explosion (Red Pawn 2)
1b	During: Assistance	Cyber assists with the attack, but may not be the primary source of vulnerability (i.e. "continues to hold the door open")	cyber control of EMS and city information systems leads to traffic jams and chaos (Green Pawn 2); Setting off chain reactions, including social chains
1c	After: Amplify	Cyber or digital means to amplify or draw attention the effects or perceived effects of a WMD after the event has occurred (i.e. "tells everyone who opened the door and what they think of it")	disinformation after nuke attack to misattribute attackers (Blue Pawn 2); Social & traditional media using misinformation, disinformation, truth, etc
1d	Ubiquitous: Falsify	When the WMD is false, but the population is fooled into believing it's true; destabilize & distract population from the true (usually non-existent event) (i.e. "tells everyone the door is open, when it's not")	False reports of chemical attack initiates evacuation order of a major city --> massive chaos follows (Neon Yellow 2)
2	Biological Hybrid	Hybrid of traditional biological WMD integrated with digital design and cyber attack; similar effects as traditional biological WMD, but new characteristics emerge from cyber capabilities of the data	Bioengineering a virus targeting only certain xenotypes or lifestyles (Neon Yellow Pawn 1); bio enabled ransomware; biological input and trigger combined with cyber attack
3	Digital Weapons of Mass Destabilization	Targeted cyber attack sets off a chain reaction of failures causing mass destabilization; usually originates in private sector (e.g. banking) or infrastructure (e.g. energy)	cyber control of EMS and city information systems leads to traffic jams and chaos (Green Pawn 2); hack on electrical grid shuts down social order reliant on IoT devices (Mint Green Pawn 3)

Note. We developed our final codebook after several passes through the data and collaboration with all the analysts.

Insights

This chapter demonstrated the standard post-analysis processes and some ways to record the connections between the raw data models and the categories of ideas that analysts find in and between models. In this demonstration, I covered the inductive steps an analyst would need to perform to justify that the analysis is complete. Then I expanded on methods, tools, and techniques to record and assist the analyst in their work. In each of

the post-analysis rounds, I described several ways to recognize how clusters of ideas form and how to identify concepts and codes within and between models. Still, I only provided a cursory look at the details in Round Three: Finding Novelty. I purposefully defer a deeper examination of the final round of post-analysis to Chapter 6. This is where I will discuss how all the minutiae of coding and clustering come together to illuminate the project's findings and how an analyst transitions from Round Three conclusions into robust findings.

I also provided examples of Professor Johnson's spreadsheet method that some analysts use to capture codes, clusters, and categories and organize their thoughts. I also identified the strengths and weaknesses of one type of qualitative analysis software that might help others. Keeping track of larger data sets becomes increasingly tedious in spreadsheet form, and I will discuss more of the benefits of software-driven analysis in the next chapter.

This case study also reveals several insights that are not listed elsewhere in the literature on threatcasting. First, this case study demonstrates the importance of Phase Zero activities, including pre-analysis research, development of the threatcasting foundation, nomination and selection of subject matter experts, and nomination and selection of participants. Since the outputs of a threatcasting project (findings, recommendations for action, and final report) are highly dependent on the set of inputs available, it was necessary to detail the work we did in Phase Zero to emphasize the importance of getting these inputs right.

Second, I introduced various methods of recording codes, transitioning them into clusters and themes, and combining ideas from several analysts into a consolidated

codebook. I emphasized process coding, concept coding, and structural coding and demonstrated they work well for the format of how data is currently recorded in threatcasting workbooks. Still, many other coding techniques are available and have a record of being highly informative to different qualitative research styles that a futurist should consider adding to their toolkit. Another important technique that I formalized in my manner of analysis is emphasizing the importance of memoing - a practice used extensively in qualitative research to record the analyst's flow of thoughts, provide a record of triggering and linking ideas, and share early insights with other researchers. Memoing in a more systematic way and memoing frequently will be necessary to future threatcasting projects that employ multiple analysts, as memos are a way to share insights and critical linking information across the team.

Third, I introduced a simplified application of Dedoose, a CAQDAS (computer-assisted qualitative data analysis software), as a tool for creating, tracking, and assessing codes, clusters, and themes. As we advance the field of foresight by demonstrating and applying successful threatcasting projects to essential questions of the future, those who use threatcasting must be ready to adapt to various data input types. I believe threatcasting analysts should become familiar with several qualitative analysis techniques, including proficiency with a qualitative software package such as Dedoose, which allows for the rapid ingestion of various qualitative and quantitative data types. I can certainly foresee a project in which mixed data analysis will be necessary to achieve a client's aims. I am also confident that proficiency in CAQDAS tools will make threatcasting that much more of a relevant methodology.

Finally, this chapter provided the first of several parts of this study's autoethnographic thread that shares “how I did it” in an attempt to inspire other futurists to be mindful of how their own processes, experiences, and worldviews impact and influence analytical findings. In this and the following case study, I exhibit the importance of the analytics attribute of thinking like a futurist. This case study is the first time anyone has recorded the processes underpinning the multiple analysts’ individual efforts into more generalizable findings that ultimately contributed to a consolidated codebook and into the first round of written conclusions. As threatcasting methodologies mature and are taught to more practitioners worldwide, the trend will be towards more collaborative post-analysis rather than solo analysis work. The activities we undertook to create that joint assessment were only the first demonstration of how a team of analysts can achieve an assessment that transcends an individual's capabilities. The case study that follows on the future of extremism in America has an even stronger examination of the power and necessity of collaborative post-analysis.

CHAPTER 5

CASE STUDY: THE FUTURE OF EXTREMISM

This chapter introduces the second of two approaches to the post-analysis process. Here I test and demonstrate three new insights into threatcasting. First is whether a hypothesis-driven methodology will provide evidence that extremism in America over the next decade will follow (or not) certain narratives of identity and whether these narratives affect the risk of radicalization towards extremism. This is the first application of hypothesis-driven analytics in a threatcasting project. Its success indicates that the threatcasting methodology is highly adaptable to the requirements of the project's research question and application areas. Second, I show additional evidence for the trend towards increasing collaboration during post-analysis. Third, I test whether models developed for previous threatcasting workshops could be repurposed to provide environmental clues and additional scenarios to anticipate the conditions in which a future threat could appear. These supplementary models helped validate our hypothesis framework and trained our analytical team before applying our hypotheses to the models purposefully created in a workshop.

Hypothesis-driven analytics indicates that a structured approach rather than an inductive approach can be used to provide guidance and helpful boundaries to newer analysts lacking experience and yet still produce critical and paradigm-shifting assessments about future threats. To test how a hypothesis investigating the relationship between narratives and extremism can be proven or validated using threatcasting, I need first to disclose the steps my analytical team took to understand the data and how we reached our findings. In essence, I am telling the story of what we did to then follow up

with a discussion about new insights into how the attributes of analytics and imagination work together to produce robust and insightful findings.

In part one, I explain the administrative and Phase Zero steps we took to form the analytical team, establish the threatcasting foundation, curate and invite subject matter experts, and invite participants to the workshop. I also discuss the strengths and weaknesses of hosting a distributed and virtual workshop, in contrast to the in-person format used for conventional events.

In part two, I describe the frameworks we chose to provide structure and boundaries to our study. This includes how my team of analysts and I agreed upon definitions, modifications to our selected narrative and radicalization frameworks, and our expectations for applying these frameworks to our data.

In part three, I explain our data collection and analysis methods. We used the raw data models from five previously published threatcasting events and scoured them for indicators of how extremism could play out by the year 2031. Although these models were not intended to support a project on extremist threats, there was sufficient detail woven into those stories that we could easily use to imagine the state of the world and extrapolate the conditions under which extremist activities could also happen. Discovering new insights into alternate uses for previously published models is an exciting step for the threatcasting methodology. I demonstrate how we used our hypothesis-driven approach to tie together years of research into a more comprehensive look at the future of extremism in America.

Finally, in part four, I describe how current events in American politics shaped the final report and how we chose to maintain boundaries on our study and avoid project

creep. This potent dose of real-world activities and media influences shaped and influenced how we used the attribute of imagination to envision the future of American extremism. The transition of power between President Trump and President Biden in late 2020 and early 2021 was exceptionally eventful. National interest in home-grown extremism rapidly increased after the Capitol Building's storming on January 6th, 2021. At a minimum, this period exposed the sores of party politics, information manipulation, and inequity that hovered below the surface of the "American identity." More importantly, it confirmed the findings we initially discovered in our data analysis, namely, that a new understanding of extremism needs to expand beyond concepts of physical violence and should include attacks on the norms and values taken for granted in the American dream. In essence, our analytical team discovered an evolutionary novel way to describe these unexplored attacks: normative extremism.

Part One: Phase Zero and a Virtual Event

In the fall of 2020, colleagues at the Pentagon contacted the ASU Threatcasting Lab to assist the Insider Threat program inside the Office of the Undersecretary of Defense for Intelligence & Security [OUSD(I&S)] with additional training vignettes for use across the Department of Defense. The Insider Threat office previously had used a threatcasting project to train employees on possible insider threat scenarios in a graphic comic named *Engineering a Traitor* (Johnson, Winkelman, & Buccellato, 2018). This graphic comic explored how a foreign nation subtly and systematically used artificial intelligence and targeted misinformation to ruin an Army officer's career and eventually

gain access to high-security computer networks. Leaders within the Department had high praise for the training value this imagined scenario provided, and they wanted more to augment their training curriculum on insider threats.

Simultaneously, the Army Cyber Institute at West Point (ACI) had several researchers looking at different types of extremism within the United States (Dawson, 2018; Dawson & Weinberg, 2020). Collaboration with the ACI and the Pentagon's request led us to believe that a project exploring the future of extremism in America using the threatcasting methodology would capture the needs of both organizations. Professor Johnson asked me to lead the project and recommended two individuals to help me with the analysis. Renny Gleeson is an experienced consultant in the creativity and marketing world, focusing on disruptive technologies and how they impact our lives, while Josh Massad is a Ph.D. student at ASU with a background in history and American politics, studying the future of technology policy. The diverse backgrounds of our project team were critical to sculpting the path to our findings on the future of American extremism, especially the characterization of normative extremism.

Similar to how we started the project on WMDs and cyber, we first developed a steering committee to define our study's scope and get input on subject matter experts and possible participants. The steering committee included researchers from ACI, a project officer at OUSD(I&S), and members of the ASU Threatcasting Lab. We again chose people with access and knowledge about extremism, insider threat, and these groups' impacts against military and government missions.

After initial research into the science of narratives and previous studies on extremism, terrorism, and radicalization, I developed a hypothesis that could be tested

with data from threatcasting models. I sketched out our hypothesis of extremism and shared it with the steering committee for further guidance. The theory is summarized as follows:

1) there exists a recognizable narrative in a person's life - call them the actor - that gives them an identity;
2) the actor is not satisfied with their current identity as described by the dominant narratives of their culture;
3) the actor seeks for and finds sympathetic narratives that reflect their desired identity;
4) there is a decision point for the actor: remain in the status quo, or embark on a journey to make a change somewhere;
5) the actor takes action (including maneuvering to gain access to resources or to enact violence) to change their environment in accordance with the sympathetic narrative;
6) their actions validate the actor's new (possibly extremist) identity.

Notice that this hypothesis is not explicitly geared towards an identity that favors or condones extremism. Until the actor possibly chooses to take violent actions in step 5, there is no indication that this theory is unique to extremist behavior. For that, we needed to find a theory about extremism and recruitment to violence in support of extremist narratives. Further discussion on this second framework follows in the section called "framing the hypothesis" and explores radicalization theories and counter-terrorism studies over the past several decades.

The chain of events suggested by this hypothesis eventually became a research question that I presented to the project's steering committee: "What are the extremist groups in America in 2031, and what stories are they telling?" The committee felt that as we begin to understand the stories that extremist groups are telling now and compare them to stories these groups might tell in the next decade, we should be able to spot whether purposeful manipulation, accidental co-opting, or social movements are

influencing the *identity* and thus the actions of those most likely to act in an extreme fashion.

This theory is supported in the literature on extremism narratives. For example, Dawson & Weinberg (2020) suggest that seemingly innocent narratives can be co-opted for complex and double-edged purposes. Contributors to the National Rifle Association's official publications changed traditional gun ownership narratives by emphasizing "strong civil religious overtones" and "elevated the Second Amendment to a sacred God-given freedom, extended the consecration from sacrifice to encompass their mainstream audience of gun owners, and identified political and cultural enemies" (Dawson & Weinberg, 2020, p. 1). Our project attempted to identify other markers of how narrative identity could be manipulated in the next decade by extremist groups. This resulted in the threatcasting foundation described in Table 2 below.

Table 2

The Threatcasting Foundation to Study the Future of American Extremism

Topic	The future of extremism in America
Research Question(s)	What are the extremist groups in America in 2031? What stories are they telling?
Application	Specific actions to disrupt, mitigate, and recover, and specific measures for the Dept. of Defense, ACI, national security apparatus (U.S. Secret Service, FBI, etc.)

The committee also recognized that we needed to collect data. A workshop on the subject of extremism in America would be an appropriate way to capture new models of the future. As we were living in a COVID-19-influenced world, we knew that a

traditional in-person workshop would not be suitable. After consulting with Professor Johnson, we decided that a virtual workshop, held in several short, highly focused Zoom sessions across the span of a week, would be acceptable to generate the models we needed.

We also had access to the raw data from several previously published threatcasting events and decided to repurpose them for several reasons. First, I knew I needed to train my analysis team on the best way to apply our framework to threatcasting data appropriately. Since our narrative and recruitment models were not designed for studying threats in the future, we had to practice and normalize the way we applied codes, categories, and themes to new and existing data in repeatable ways.

Second, I needed to discover whether previous data could be mined for new insights beyond their original scope. Professor Johnson had theorized that our corpus of threatcasting reports contained actionable and valuable insights into futures outside the immediate application areas they were developed for, but he had not yet had a project in which to prove this. He suggested I use all available models to test the idea.

Finally, the third reason to use existing models in addition to creating new ones was to broaden our set of plausible scenarios to minimize the narrowness of vision inherent in using a limited group of participants to generate models. Even though a typical workshop can develop 20-40 unique models on a particular topic, we knew that a constrained virtual workshop would have fewer participants. This meant there would be fewer opportunities to stretch the imaginative limits of our participants. Additional models would improve the variance in imagination and different perspectives, which should help fill in blind spots that naturally occur in a workshop.

Part Two: Framing the Hypothesis

In order to use a hypothesis-driven approach, our project team first had to understand the research already available on the topics of extremism, recruitment, and radicalization as well as narratives, storytelling, and identity. We investigated far-right extremism in the United States (Jones, 2018); lone wolf radicals - including arguments that the lone wolf typology is misconceived (Hauck, 2020; Hunt, 2013; Schuurman et al., 2019); female jihadists in America and whether the identity of being a woman was a factor in radicalization (Alexander, 2016); the spread of radicalization in the United States (Smith, 2018); and government efforts to counter terrorism and other targeted violence (Department of Defense, 2012; Department of Homeland Security, 2019). We found a study commissioned by the U.S. Army's Asymmetric Warfare Group (AWG) (Crossett & Spitaletta, 2010) investigating radicalization's psychological and sociological concepts. This framework closely aligned with indicators of violent radicalization we observed in threatcasting models from previous projects. We then adapted the sixteen radicalization risk factors from the AWG study for our use. The radicalization framework categories and their definitions explain how to apply them to our threatcasting models (see Appendix A).

We also needed a framework to understand narratives and how to analyze them. This is particularly relevant to understand how narratives connect to the identity and motivations of people who find extremist violence a viable course of action. We reached into classical narrative identity studies such as those by Francesca Polletta (Polletta, 1998b, 1998a; Polletta et al., 2011) and epistemic dependence by John Hardwig

(Hardwig, 1985). We also looked for guidance from researchers investigating the intersection of narratives and violence (Corman, 2016; Fine, 1999; Maan, 2015) and how people use print magazines, social media, and modern communication to broadcast and distribute narratives supporting violence (Benigni et al., 2017; Dawson & Weinberg, 2020). We also researched how FICINT, or fictional intelligence that "melds narrative and nonfiction," could help us bridge narratives and imagined futures (Cole & Singer, 2020). Work by Dan McAdams and Kate McLean (2013) on narrative identity ultimately provided us a workable framework of seven life-story constructs that we adapted for our research.

The narrative categories developed by McAdams & McLean researched the relationship between life stories and how individuals adapted to changes (see Appendix B). In these changes, "People convey to themselves and to others who they are now, how they came to be, and where they think their lives may be going in the future" (McAdams & McLean, 2013, p. 233). We used the authors' definitions as written and applied them to our models by imagining how the story's protagonist attempted to act. We adapted these constructs to investigate whether extremist behavior could be a possible narrative that people would adopt into their identities under certain circumstances.

After discussing with my analytical team what the two frameworks separately provided and how to define each term and category, we then discussed how to best apply them together as a single framework. This allowed us to test our hypothesis about the identity shift that should appear in stories of extremism. We first discussed two or three scenarios in-depth and identified when it would be appropriate to assess whether to apply one or more identity constructs and which one would be dominant if there were multiple

constructs present. For instance, the protagonist in a model might act to achieve "Redemption" to salvage a bad situation through violence. In actuality, the underlying identity conflict was a discrepancy of "Agency" or the perceived lack of freedom to make the changes necessary to achieve success.

We also ensured our definitions of the radicalization risk factors were precise enough to tell the difference between similar risks. For instance, a "non-negative view on violence" is quite similar to "the perceived benefit of violence," yet they are subtly different categories that we needed to clarify. We felt the former was best described as the acculturation of violence through media, movies, video games, and other factors that made violence more acceptable. Simultaneously, the latter was best applied as a circumstance of last resort to solve problems.

We had similar discussions on the nuances of "resources" and "external support." To us, "resources" were the materials and financial support needed to further action, whereas "external support" was a category of intangible benefits, usually from a benefactor, and it expressly excluded the funds and materials needed for action.

Once the three of us had our yardsticks calibrated, we set off to separately investigate the models and see how our experiences, worldviews, and biases might produce different outcomes, given the same inputs. I asked the team to individually assess the data using the same frameworks for three reasons. The first was to test the strength of the interrater reliability factor that is important to qualitative analysis legitimacy and ensure that it applies to analyzing imagined futures and threatcasting models. I suspected that we would not use the exact same codes for all the models, but it would be close because we had spent a session normalizing our definitions and terms.

After the first round of coding for identity constructs and radicalization risk factors, we again gathered to ensure we had similar views. We found we had approximately 96% interrater reliability after recalibrating a couple of outlier models from the priming data set.

The second reason for independent analysis was to allow for a freshness of perspective that prevents one analyst's point of view from dominating the conversation. I wanted to establish an environment where personal experiences and worldviews would be visible in an analyst's work. Again, bias and points of view within threatcasting are features and not flaws, but only so far as they are visible and above board. Hidden agendas, overbearing personalities, or inattentiveness may lead to unfounded results without a way to understand where we went astray or how to correct for these types of biases.

Finally, the third reason for independent work was so that each person could work through the post-analysis alone first and exercise the muscles required to complete the post-analysis steps, leading to a set of findings. I needed my analysts to exercise their analytical powers because I would later solicit their input for a separate project on assessing creativity as a requirement to think like a futurist. This project required each futurist to independently assess the same data without the ability to converse with each other or calibrate their yardsticks. I demonstrate the project's results in Chapter 6 when I investigate the imagination attribute of thinking like a futurist.

Part Three: Data Collection and Methods of Analysis

The data available to this project consisted of two blocks. The first, called the priming data set, was from five previously published threatcasting workshops and reports. Although these models originally answered their particular studies' research questions, they helped us in several ways. The first was to help visualize and understand the social, political, and technological conditions that may exist prior to or during a violent extremist act. These conditions also described recruitment trends, radicalization pathways, and how attacks on social norms were developing over time. Second, the priming data also provided additional possible and probable futures in which violence manifested and allowed us to consider whether we could attribute violence in these scenarios with extremist narratives or identities that promote extremism. Finally, using previous data gives confidence to the Threatcasting Lab that data have additional longevity beyond their original collection and might be valuable for many future projects yet to be imagined.

Table 3 lists all the workshops and the abbreviations we used, and the number of models available in each report. The last report listed, “The Future of Extremism in America” (abbreviation: EXTR), contains the models from the virtual extremism workshop and is the second block of data we needed for our analysis.

The first step in our analysis was to filter the priming data (n=122) for models that did not have sufficient detail to help our study of extremism or were outside the boundaries. Since our focus was on extremism in the United States, we had to create a

boundary condition that took geography into account. This included political geography and motivations of actors as well as physical geography.

Table 3

Threatcasting Models Available for Analysis

Abbreviation	Report Content	# of Models	Citation
WEST	Future of Cyber Warfare (Threatcasting West)	n=22	Johnson, 2016
ACI	Future of Weaponized Artificial Intelligence	n=14	Johnson et al., 2017
IDM	Information Disorder Machines	n=24	Johnson, 2019
IW	Future of Information Warfare	n=18	Johnson et al., 2020
DTRA	Future of Cyber and Weapons of Mass Destruction	n=44	Johnson, Brown, et al., 2021
EXTR	Future of Extremism in America	n=12	Brown et al., 2021

Note. We ended up with a combined data set of 52 models useful for further analysis, 40 from the priming data and 12 from the extremism workshop.

For the most part, we excluded models that included nation-state actors or nation-state proxies as the antagonist, even if they supported, directed, or enabled violent actions within the U.S. borders. We decided these motivations were typical of traditional statecraft and political conflict, making it difficult to distinguish the threat and their actions from categorically "true" extremists.

In the same vein, we excluded threat actors that were primarily criminal in nature. Gangs, drug cartels, and criminal organizations occasionally appeared in the priming

data, but we assessed their actions, regardless of whether they were violent or not, as typical of meeting the goals and aims of criminals: largely for-profit and self-serving end states. The models we had in the priming data demonstrated violence from criminal organizations but did not display *identities* in line with extremism.

Of course, there are always exceptions to a hard-and-fast boundary rule. A fuzzy boundary for one model included state-sponsorship as a supporting actor to a criminal organization. WEST Team 11-2 imagined a Sinaloa drug cartel paying Russian and Chinese state-supported hackers to compromise and exploit social media platforms to influence American youth to sell drugs for profit. We found that in the scenario, hackers used automated software and algorithms to create a self-funding "flywheel" that automatically generated revenue for both the foreign hacker groups and the drug cartel. This was one of the first instances of corporate extremism or extremist actions to pursue economic goals (profit) rather than political or social purposes. This idea would become the core of one of our findings surrounding corporate extremism.

This means that we created a filter to look at both the effect and the intent of those perpetrating violent actions. Looking at only violence as a qualifier for extremism ignores the purpose and motivations of actors; looking at just intent or motivations does not meet the threshold of our agreed-upon definition set by the FBI that must include violence. This reinforces why we chose to look at violence from the perspective of narratives and how they tie to identity. Narratives of state-on-state conflict or criminal violence-for-profit are different than the narratives of people seeking to live normal lives. Whether these people are U.S. citizens, immigrants, tourists, or businessmen and women from abroad, the American birthright suggests that these individuals have a reason to be

normally law-abiding and act in accordance with social norms instead of seeking violence to rectify any identity conflict they may have. At least, that is what our hypothesis suggested.

The corollary to our hypothesis suggested that someone radicalized to violence has an identity that has begun moving away from expected social norms out towards a fringe position where two choices present themselves. Either they willingly choose violence to rectify an identity conflict, or they feel they have no option *but* to choose violence as a means to resolve the dissonance in their identity. And this is precisely what we found within the data.

The next step in our curation of the data was to review each model from the priming data and see if it fell within our new boundaries. Of the 122 models in the five priming workshops, we ended up with 40 violent or extremist-oriented threat models that included extremist markers.

We then coded each model with the type of narrative identity (Con, R, A, E, CPR, Comm, M) corresponding to the primary narrative the *threat actor* was trying to achieve. Although threatcasting suggests we develop models from the perspective of a person, in a place, experiencing a threat, we recognized there was enough data to understand the threat actor or threat group's narrative and internal identity. In some models, the protagonist experienced the threat future in such a way that they became the threat actor or extremist, in which case the narrative of the threat and the protagonist became the same. In other situations, the *story* of the threat suggested one type of identity (e.g., the story looked like a redemption identity), but the actual *narrative* was different (e.g., Agency was, in fact, the identity that was in conflict). We also looked for the presence of

the radicalization risk factors and coded them one through sixteen, as listed in Table ###. This constituted our first round of coding, corresponding to threatcasting's "Round One: Summarizing" of the post-analysis phase.

Next, we met again to normalize our first round of coding. The three of us discussed which identity construct was most applicable to each model. In cases where we could clearly distinguish between the narrative of the threat and the narrative of the model's central character, we coded the model with both if they were different. At this point, I asked each analyst to do the same first-round coding of the 12 new models we developed at the extremism workshop. I then asked them to continue through to the second round of coding to try and ascertain the meaning (post-analysis "Round Two: Finding Meaning") and high-level findings ("Round Three: Finding Novelty") of the combined data set.

Each analyst used their own way to apply and track codes. Renny and Josh used Google Docs and Google Sheets, and I chose to use the software program, Dedoose. Because of the software, I was able to produce a code co-occurrence matrix that compared the number of times a code appears in the same model as another code. What was relevant to our study was the intersection of the identity construct codes and the radicalization risk factors and how many of the radicalization risk factors were present simultaneously. Since we usually identified a single identity construct for each model, it was unnecessary to look at how often they overlapped. As far as I can tell, this is the first time any threatcasting analyst has used a code co-occurrence matrix to augment their analysis.

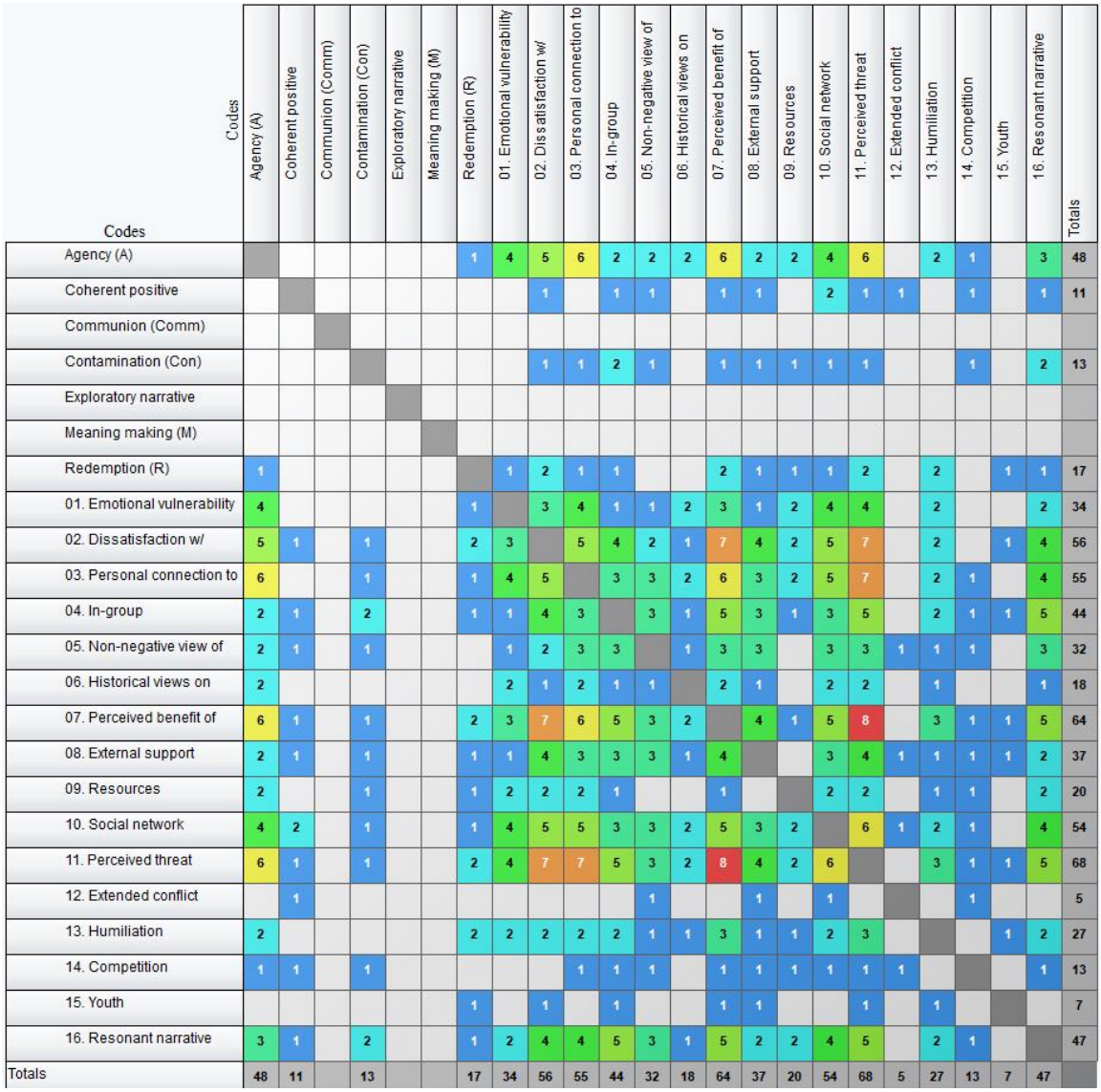
Figures 9 and 10 illustrate two such matrices. Darker yellow and red numbers indicate a higher co-occurrence between the two codes. The first matrix is the co-occurrence in just the data from the 12 models from the extremism workshop. This matrix helped visualize what risk factors were essential and which identity construct was most prevalent in models specifically designed to assess extremist futures. In this matrix, "Agency" was the most frequently observed narrative identity construct. "Personal connection with a grievance," "Perceived benefit of violence," and "Perceived threat," each with (n=6), suggested that an extremism narrative was convincing to an individual when their own lives were affected by something outside of their control. "Dissatisfaction with the status quo" appeared twice as the highest co-occurring code (n=7) alongside "Perceived threat" and "Perceived benefit of violence" when assessing the risk of radicalization. This suggested that radicalization to extremist action is most likely to occur when a person feels some type of dissatisfaction with the way the world operates. Additionally, the threat to a person's way of life was most potent when it caused personal trauma, fear, anxiety, loss, or other grievance. People who felt personally attacked by "the system" or who had been wronged somehow were more likely to turn to violence when there were no other options left.

The second image (Figure 10) is the co-occurrence of all 52 models aggregated together. The co-occurrences were not the same, suggesting that environmental factors (e.g., political, economic, social, technological, etc.) were more detailed in some of our priming data that were not present in our extremism models. "Agency" remained the leading identity construct, and we assessed this again to mean the narrative was, in fact, a *lack of* agency that was the center of a person's identity conflict. Although

"Dissatisfaction with the status quo" remained the most frequent radicalization risk factor, this time, it occurred more frequently with a "Non-negative view of violence.".

Figure 9

Extremism Workshop Code Co-Occurrence

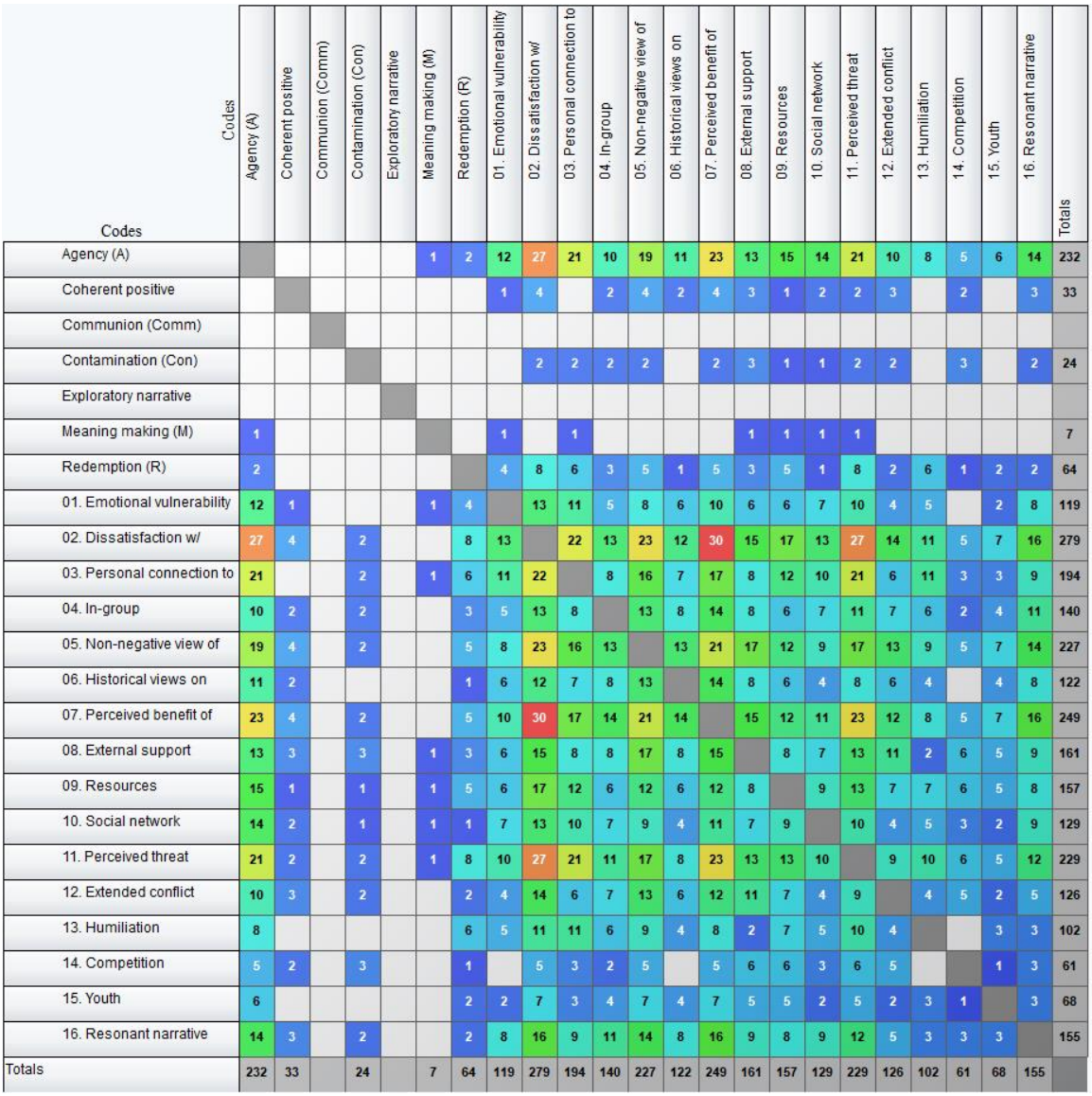


Codes	Agency (A)	Coherent positive	Communion (Comm)	Contamination (Con)	Exploratory narrative	Meaning making (M)	Redemption (R)	01. Emotional vulnerability	02. Dissatisfaction w/	03. Personal connection to	04. In-group	05. Non-negative view of	06. Historical views on	07. Perceived benefit of	08. External support	09. Resources	10. Social network	11. Perceived threat	12. Extended conflict	13. Humiliation	14. Competition	15. Youth	16. Resonant narrative	Totals
Agency (A)							1	4	5	6	2	2	2	6	2	2	4	6		2	1		3	48
Coherent positive									1		1	1		1	1		2	1	1		1		1	11
Communion (Comm)																								
Contamination (Con)									1	1	2	1		1	1	1	1	1			1		2	13
Exploratory narrative																								
Meaning making (M)																								
Redemption (R)	1							1	2	1	1			2	1	1	1	2		2		1	1	17
01. Emotional vulnerability	4						1		3	4	1	1	2	3	1	2	4	4		2			2	34
02. Dissatisfaction w/	5	1		1			2	3		5	4	2	1	7	4	2	5	7		2		1	4	56
03. Personal connection to	6			1			1	4	5		3	3	2	6	3	2	5	7		2	1		4	55
04. In-group	2	1		2			1	1	4	3		3	1	5	3	1	3	5		2	1	1	5	44
05. Non-negative view of	2	1		1				1	2	3	3		1	3	3		3	3	1	1	1		3	32
06. Historical views on	2							2	1	2	1	1		2	1		2	2		1			1	18
07. Perceived benefit of	6	1		1			2	3	7	6	5	3	2		4	1	5	8		3	1	1	5	64
08. External support	2	1		1			1	1	4	3	3	3	1	4			3	4	1	1	1	1	2	37
09. Resources	2			1			1	2	2	2	1			1			2	2		1	1		2	20
10. Social network	4	2		1			1	4	5	5	3	3	2	5	3	2		6	1	2	1		4	54
11. Perceived threat	6	1		1			2	4	7	7	5	3	2	8	4	2	6			3	1	1	5	68
12. Extended conflict		1										1			1		1				1			5
13. Humiliation	2						2	2	2	2	2	1	1	3	1	1	2	3				1	2	27
14. Competition	1	1		1						1	1	1		1	1	1	1	1	1				1	13
15. Youth							1		1		1			1	1			1		1				7
16. Resonant narrative	3	1		2			1	2	4	4	5	3	1	5	2	2	4	5		2	1			47
Totals	48	11		13			17	34	56	55	44	32	18	64	37	20	54	68	5	27	13	7	47	

Note. Code co-occurrence matrix from only the extremism workshop data.

Figure 10

Combined Data Code Co-Occurrence



Codes	Agency (A)	Coherent positive	Communion (Comm)	Contamination (Con)	Exploratory narrative	Meaning making (M)	Redemption (R)	01. Emotional vulnerability	02. Dissatisfaction w/	03. Personal connection to	04. In-group	05. Non-negative view of	06. Historical views on	07. Perceived benefit of	08. External support	09. Resources	10. Social network	11. Perceived threat	12. Extended conflict	13. Humiliation	14. Competition	15. Youth	16. Resonant narrative	Totals
Agency (A)						1	2	12	27	21	10	19	11	23	13	15	14	21	10	8	5	6	14	232
Coherent positive								1	4		2	4	2	4	3	1	2	2	3		2		3	33
Communion (Comm)																								
Contamination (Con)									2	2	2	2		2	3	1	1	2	2		3		2	24
Exploratory narrative																								
Meaning making (M)	1							1		1					1	1	1	1						7
Redemption (R)	2							4	8	6	3	5	1	5	3	5	1	8	2	6	1	2	2	64
01. Emotional vulnerability	12	1				1	4		13	11	5	8	6	10	6	6	7	10	4	5		2	8	119
02. Dissatisfaction w/	27	4		2			8	13		22	13	23	12	30	15	17	13	27	14	11	5	7	16	279
03. Personal connection to	21			2		1	6	11	22		8	16	7	17	8	12	10	21	6	11	3	3	9	194
04. In-group	10	2		2			3	5	13	8		13	8	14	8	6	7	11	7	6	2	4	11	140
05. Non-negative view of	19	4		2			5	8	23	16	13		13	21	17	12	9	17	13	9	5	7	14	227
06. Historical views on	11	2					1	6	12	7	8	13		14	8	6	4	8	6	4		4	8	122
07. Perceived benefit of	23	4		2			5	10	30	17	14	21	14		15	12	11	23	12	8	5	7	16	249
08. External support	13	3		3		1	3	6	15	8	8	17	8	15		8	7	13	11	2	6	5	9	161
09. Resources	15	1		1		1	5	6	17	12	6	12	6	12	8		9	13	7	7	6	5	8	157
10. Social network	14	2		1		1	1	7	13	10	7	9	4	11	7	9		10	4	5	3	2	9	129
11. Perceived threat	21	2		2		1	8	10	27	21	11	17	8	23	13	13	10		9	10	6	5	12	229
12. Extended conflict	10	3		2			2	4	14	6	7	13	6	12	11	7	4	9		4	5	2	5	126
13. Humiliation	8						6	5	11	11	6	9	4	8	2	7	5	10	4			3	3	102
14. Competition	5	2		3			1		5	3	2	5		5	6	6	3	6	5			1	3	61
15. Youth	6						2	2	7	3	4	7	4	7	5	5	2	5	2	3	1		3	68
16. Resonant narrative	14	3		2			2	8	16	9	11	14	8	16	9	8	9	12	5	3	3	3		155
Totals	232	33		24		7	64	119	279	194	140	227	122	249	161	157	129	229	126	102	61	68	155	

Note. Code co-occurrence matrix from the historical data and extremism workshop data.

Recall that a non-negative view of violence comes about by acculturation and constantly living with violent situations. This means that the next decade's environment will continue to portray violence as routine rather than as something abhorrent. It is also

interesting to note that we observed relatively few instances of "Historical views on violence" co-occurrent with either "Agency" or any radicalization risk factors. Recall that we took a historical view on violence to mean a situation in which someone has used violence before to solve a problem. This suggested that when a person turned to violence as a last resort, they did so usually for the first time! They had exhausted all avenues of rectifying their dissatisfaction with the status quo, or at least believed they had, and violence became the only practical solution.

After the first round, we (excitedly) began to see differences in opinion on what more profound findings lay underneath the application of framework codes. We found that these differences in opinion stemmed from the analytical teams' different backgrounds, life experiences, and world views. These differences also closely aligned with varying degrees of emphasis on whether analytics, imagination, or responsibility was dominant in applying our perspectives to the data. What was most interesting was how we learned from one another about different worldviews. We stuck to finding the most suitable assessment that fit all our understanding rather than the "best" assessment. We realized that a "best" assessment was unrealistic given threatcasting's emphasis that people (and their inherent differences) are a design feature rather than a design flaw. True objectivity is rather unhelpful in assessing deeply seated emotional and socially entrenched values such as those that influence the identities of people reaching for violence when other ways of reconciliation seem to fail.

Part Four: Discovering a New Understanding of Extremism

In the successive rounds of analysis, or rather "Round Two: Finding Meaning" and "Round Three: Finding Novelty," we each created clusters of ideas coded from *in vivo* statements, concepts, and processes that we observed in and between models. We then categorized them into more abstract and higher-level groups to find three distinct topics that were of interest in the end. The first was about corporate extremism or the idea that corporations, in their pursuit of profit and market ownership, took actions that were not overtly violent but instead promoted social conflict in their marketing, advertising, or business practices that sometimes led to violence.

The second finding was that algorithms would be used to amplify political and social tensions. A growing trend of "digital violence" perpetrated through social media would include things like character assassination, monetization of truth and facts (or alternate facts), and the rise of deep fakes for political gain. The realization that some of the same corporate power structures that activated corporate extremism in pursuit of profits also controlled many of these algorithms was a disturbing reinforcement of the subtlety of the damage corporate extremism could have on American society.

The last high-level finding we labeled at first "Fighting for the American Dream," and it captured the idea of people's frustration and dissatisfaction with their inability to follow, let alone achieve, life, liberty, and the pursuit of happiness. Our data suggested a growing sense that personal agency was being taken away (by whom was not always clear, but most models pointed fingers at the government). Our previous categories suggested it may even be done by automated programs or on behalf of profit-following

corporations. However, the “fight” for the American dream was only part of the answer. After several more conversations, we had a moment of clarity that led to discovering something genuinely novel - something that the data did not directly reveal but was only visible after applying the biases, experiences, and worldviews of human analysis.

I was discussing with Renny Gleeson some edits we needed to make after releasing our first draft to participants for peer review. Renny was concerned about the lack of clarity on actions we could recommend for recovering from an extremist event. Since providing recommendations for action is part of the threatcasting foundation, we needed to dig deeper. We already included several suggestions that gatekeepers could take to prevent or mitigate extremism's effects *before* a violent event happened. These included monitoring cryptocurrency transactions between suspected extremist organizations or studying the encrypted communication platforms between members of such organizations. Granted, some of these recommendations would be useful in the recovery phase, but there were very few references in the models explicitly crafted for gatekeepers to use *after* the fact.

Initially, this indicated to me that there are two weaknesses in the threatcasting process. The first is that backcasting, or the part of the process in which participants consider the gates and flags and imagine what can be done about them, is traditionally not given sufficient time or attention to thoroughly completing the analysis during a workshop. Indeed, having experienced several workshops as a participant and several as an analyst, I noticed the thinness or lack of depth in the workbooks where there is space to ponder and discuss what should be done. This is not a flaw of the methodology;

instead, it is because backcasting is quite hard to do correctly. The emphasis of a workshop is usually to generate many diverse models rather than perfecting just a few.

The other apparent weakness, especially in recommending what to do about recovering from American extremism, is based on our perceptions of the gatekeepers' feasible actions. Recall that the threatcasting foundation starts with some vision of how gatekeepers will apply the results. We originally had the military and government writ large in mind as gatekeepers when we crafted the application areas: How can the Department of Defense recognize an insider threat? What can the U.S. government do to detect occurrences of extremism recruitment, radicalization, and mobilization to action? Or, how should academia focus on research to learn more about the narratives that cause people to gravitate towards the fringe? These types of questions suggested the application scope for our foundation.

What we were excited to realize when discussing our understandably thin set of recovery recommendations is that we had stumbled upon a new set of findings - one that immediately shouted to us, "this is what our findings *really* point to!" At the time of writing the extremism report, the U.S. was experiencing first-hand the aftermath of the January 6th, 2021 storming of Capitol Hill, and we were literally living in the recovery from those events. What could we learn from observing the state of the world around us? We reflected on the prosecution reports of those involved in the events on Capitol Hill. We could sense that many people, from citizens up to elected officials, were seeking - no, demanding - some type of justice for those who incited and coordinated a violent event, stormed the capitol, and trashed symbolically important norms within the American

dream. Justice was an avenue to reestablish a normative feeling of fairness by prosecuting those who trespassed and trampled on politically sacred ground.

This was when both Renny and I realized that "ah-ha!" moment that there was something more to this recovery phase than we initially thought. We recognized that justice through prosecution could only satisfy the legal fairness established by written and enforceable laws. But what about satisfying the fairness of norms or culture? Would additional regulation about the criminality of storming the Capitol Building help people feel more or less vindicated?

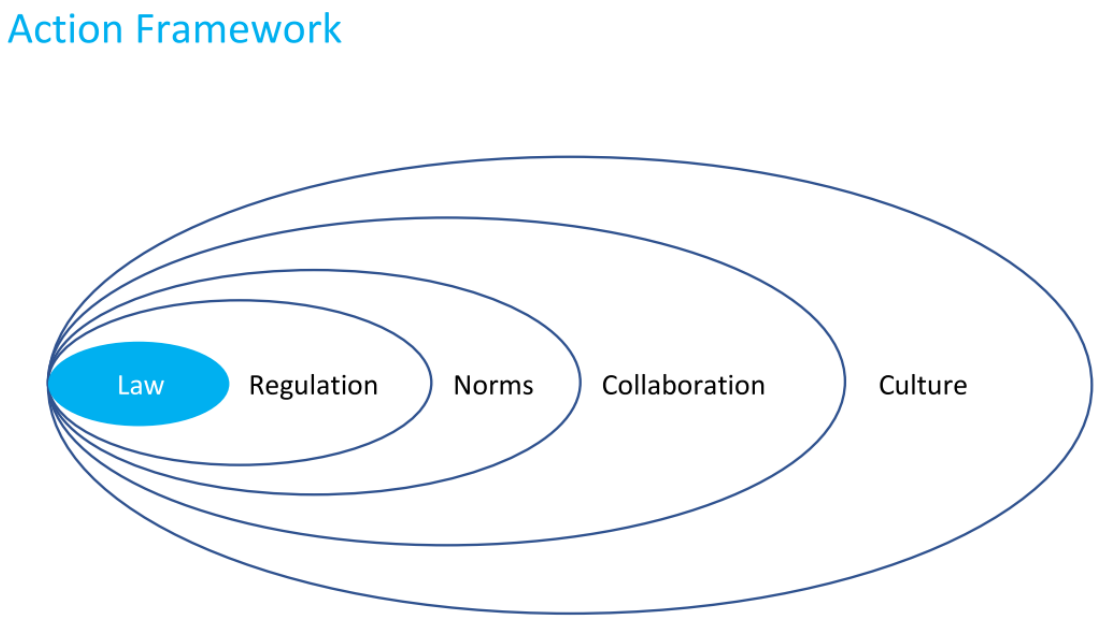
I then brought out a diagram and another framework for action that the Menzies Foundation recently published in their report on the future of risk, security, and the law. The Menzies Foundation is an Australian group focused on fostering a better understanding of leadership for 21st century Australia. Their report suggests that action plans have overlapping and nested circles of responsibility, and legal responsibility lies in a small circle in the center. In contrast, cultural responsibility for action encompasses a much broader swath of possible actions (see Figure 11).

We realized there was a growing attack on the norms that glue together American culture and American laws. What we were observing was a type of "normative extremism" that attacked the very ideas underpinning the American Dream. Because much of normative extremism is not violent, the indicators fell beneath the threshold of the FBI's definition and would typically escape our radicalization filter. Normative extremism attacks the area between laws, regulation, and culture, making it fall beneath the legal radar. Neither does it stir the hornet's nest of patriotic fervor by avoiding a direct attack on the underlying culture. But what normative extremism does not do is

escape the filter of narrative identity, especially as it pertains to the agency identity construct. In every instance that our models suggested there was a conflict between what someone wanted to do and their inability to achieve it, we observed some external attack on cultural norms and the idea of what it meant to achieve the American Dream!

Figure 11

Menzies Foundation Action Framework



Note. Normative extremism attacks the area between laws/regulation and culture, making it fall beneath the legal radar and avoiding a direct attack on the underlying culture. Adapted from Menzies Foundation (2020, p. 11). Used with permission.

For example, Team Blue 2 told the story of Matt, who is a member of Techno-Jihad, a religious group that believes the end of the world is natural but is not coming

soon enough. One of the principles of Techno-Jihad is that their group should accelerate the end of the world by attacking critical technology sources such as the U.S. energy infrastructure, hoping that its collapse will save humanity by speeding up the apocalypse (Brown et al., 2021). By attacking critical infrastructure as a religious target, Techno-Jihad indirectly attacked the norms, or guiding principles, that religion should be about perfecting the individual and coming to terms with one's purpose in life. Instead, Techno-Jihad attempted to replace these norms with principles of excusing mass human suffering for the sake of saving the planet.

The new perspective on how the definition of extremism could now encompass a systematic attack on norms was such a substantially evolutionary idea that we reworked the category of "Fighting for the American Dream" to become "Rise in Normative Extremism." We also set a schedule for following up on the idea in future research and additional publications.

Insights

What this case study primarily demonstrates is that thinking like a futurist can be done with the aid of existing frameworks, using a hypothesis-driven approach. I have shown how I searched through existing literature on extremism, radicalization, violence, narratives, and identity to find two acceptable frameworks appropriate to apply to threatcasting data. I showed the relevance of using previously published threatcasting models in studies beyond their original intention, giving additional longevity to the hard work done in other studies. I also demonstrated the usefulness of both individual and collective analysis to capitalize on both techniques' strengths. In fact, we could not have

achieved such powerful results without bringing together the strengths of having analysts with diverse backgrounds and life experiences. Finally, I demonstrated how qualitative analysis software could develop additional insights into data analysis that are extremely difficult to do by hand.

I also have several observations from this case study that changed my understanding of the threatcasting methodology, which helped me become a more proficient futurist. First, I noticed that backcasting remains a weakness in the threatcasting methodology. This may be due to insufficient time and attention given to this step during model creation, or it may be that there is too much openness in responding to the workbook prompts that ask for participants to recommend gates and flags. On the other hand, it is quite serendipitous that we did not have a robust backcast with fully developed recommendations for action to give to our client. This was one of the weaknesses of hosting the workshop virtually. I could not facilitate every small group meeting and provide clarification or guidance about backcasting's requirements or format since each group used their own schedule to work.

The serendipity appeared because of this lack of clarity, which then forced us to reflect on both the current events surrounding the storming of Capitol Hill and seek external guidance about where to place the shock of that event in our world view. To do that, we adopted a paradigm developed by an Australian think-tank that suggested there are overlapping spheres of responsibility to take action. At the center are laws and regulations that formalize the acceptable activities to take in well-defined circumstances. At the outer ring are social constructs that use slow-moving cultural changes to affect public, private, and individual responses to risks and threats (Menzies Foundation, 2020).

And in between laws and culture are normative forces that guide, influence, and compel people to take action in specific ways so that they remain within acceptable bounds informally established by the "group." Without the Menzies Foundation's action framework visualization, we may have missed the evolutionary shift and rise of normative extremism that our data suggested would increase over the next decade.

In order to improve the quality of backcasting data, I suggest the following several modifications to the threatcasting framework. First, during a workshop, emphasize a narrower understanding of gatekeepers initially. The first set of gatekeepers that should receive recommendations for action are the clients and primary recipients of the threatcasting report. If there is additional time, have participants return to backcasting for action items to recommend to a broader range of gatekeepers and follow the Menzies Foundation's action framework for categories of these groups. Legal and regulatory recommendations are the most direct, followed by normative gates that improve self-regulation and consider collaboration action items that span organizations, domains, and other areas of expertise. Finally, recommend cultural shifts that, if adopted, would assist the primary gatekeepers in avoiding, mitigating, or recovering from threat futures.

The second suggestion for improving the quality of models and subsequent findings is to schedule a separate backcasting work session with the primary gatekeepers (e.g., the client) to explore in-depth a selection of the best and most plausible scenarios from the first workshop. This was done with great success in the project on information warfare and the future of conflict (Johnson et al., 2020). Shortly after our team of futurists completed the first round of post-analysis on this project, facilitators from the Threatcasting Lab traveled to the Naval Postgraduate School (NPS) at Monterey, CA, to

gather additional insights into how the Department of Defense could further avoid, mitigate, or recover from the threats of information warfare. A small group of currently serving military officers and academics from NPS spent a day reviewing and discussing specific responses to two of the models developed in the first workshop.

This second session recommended five areas of action and operationalization, including understanding the decay of the American "brand," understanding the limitations of plans to control the narrative, ways to protect the force, ways to counter the tide of soft power, and strategies to implement disruption and delaying principles into U.S. information warfare plans (Johnson et al., 2020). These insights would not have been as clear without a separate backcasting session.

A focused backcasting session may not always be logistically feasible to hold in-person, so futurists should consider the strengths and weaknesses of hosting a virtual session such as the one described in the case study in this chapter. An alternative suggestion is to informally gather at least one other futurist and spend a lunch hour scrutinizing a few models for better and more accurate application areas. At a minimum, this provides at least some measure of robustness in the backcasting phase and helps patch some of the more obvious gaps in the data, including places where workshop participants left these data blank.

Next, I discovered how to use data from previous workshops to provide our analysts a broader perspective on the conditions and environments that many people have imagined the future to hold. One of the maxims of foresight work is that the future will not be much different from what it is today. The other is the notion that "the future is built by people" (Johnson, 2021, p. 93). Although we take great care to consider wildly

imaginative futures and the threats that might appear in them, the actuality is regardless of the threat, the underlying social, political, technological, and environmental conditions move pretty slowly. We can learn as much about the anticipated future conditions of the world from a model created for the future of information warfare or the future of artificial intelligence as we can from a model developed for the future of extremism. This is even more true the closer the projects are to one another. Computer algorithms using infinite amounts of our personal data can make pinpoint recommendations about what news feeds we see or don't see or what political groups appear at the top of our social media inboxes. This information might even incite someone to follow a path toward extremism. There is an interconnected web of forces that weave through many of the threatcasting reports we pulled from to get our priming data. Each model we selected described a nuance of the environment that helped us better understand how narratives, identity, radicalization, and opinions on violence meshed together to move someone to extremist activities. Repurposing previous models was an important experiment for the future of threatcasting that should continue to be explored by other researchers in other contexts.

Lastly, I learned about the importance of collaboration and relying on other futurists' experiences and worldviews to make a more thorough and nuanced product. Our analytical team met at least a half-dozen times over four months to refine our techniques and balance the yardsticks we used to measure the data against our framework. Each time we met, we had specific goals to achieve by the end of the meeting and responsibilities to finish before the next scheduled meeting. Some of these meetings included refining and adapting our codebook. Others were in-depth discussions on the differences between nation-state actors, proxies, criminal groups, and the general public's views on violence

and whether extremism was internally or externally motivated. At other times we discussed research from news reports and academic journals on the rise of corporate extremism, mainly focusing on prominent social media companies and their practices to allow, monitor, or censor certain types of speech and online behavior. Each of these meetings helped us refine and more broadly generalize the future of extremism in America and ultimately allowed us to develop the initial roots on the idea of normative extremism.

CHAPTER 6

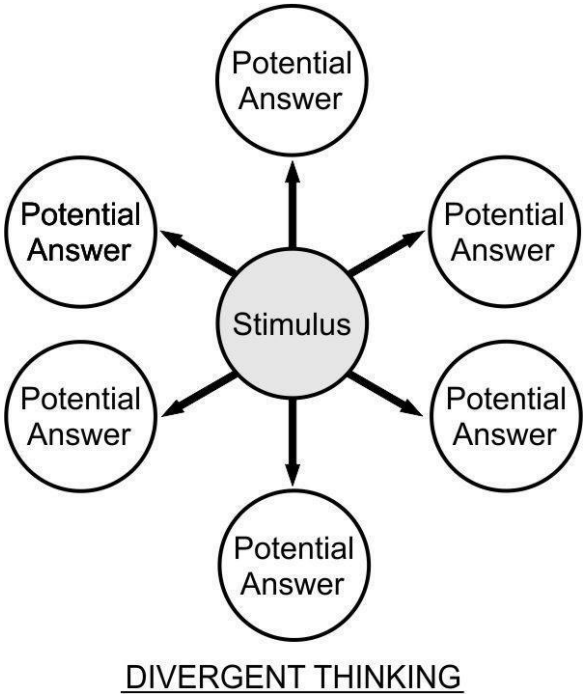
INVESTIGATING NOVELTY

Divergent Versus Convergent Thinking

Imagining future threats celebrates divergent thinking, creativity, and inspecting threats in new ways, which is why threatcasting seeks diverse opinions and a broad reach of participants for a particular problem or project. When workshop participants generate fictional scenarios about a future threat using randomized inputs, they practice divergent thinking. Figure 12 illustrates divergent thinking through a map showing a central stimulus generating multiple answers that are not connected in any immediately clear way with each other. For threatcasting, the central stimulus is not a simple research question or brainstorming prompt. Instead, it is the aggregate of the synthesized workshop inputs from subject matter experts, pre-analysis research prompts, and the culmination of careful participant curation. While the pattern of potential answers depicted in Figure 12 appears to be evenly distributed and is ideally the best spread to ensure a fair imagining of the future, in reality, participants tend to create scenarios that congregate into a similar range of futures. For now, the extent of this clustering is anecdotal but can be observed in the style of scenarios developed during each futurecasting round. Further research on the make-up and backgrounds of participants measured against the styles of scenarios they tend to produce would be necessary to determine if there are measurable gaps in the types of futures that threatcasting tends to evaluate. I leave that analysis to a future project.

Figure 12

Divergent Thinking



Note. Licensed under Creative Commons Attribution-Share Alike 4.0 International (Aishwarya.gudadhe, 2015).

To demonstrate this clustering, I briefly return to the case study investigating the future of weapons of mass destruction and cyber. In the first round of modeling, participants in that workshop generated fifteen scenarios. Eleven clustered around the effects of some variation of a genetically modified virus or biological vector targeting specific groups or individuals (Johnson, Brown, et al., 2021). Facilitators at the event recognized the influence of current events since, at the time of the workshop, COVID-19

was beginning to spread around the world. The idea of a weaponized version of a virus was very likely in participants' minds, and they rightly wanted to explore the future of this type of threat. Facilitators then requested that participants diverge their scenarios to consider other weapons of mass destruction in subsequent modeling rounds. They asked for additional diversity not because they wanted to stifle the creativity of participants but because they needed to provide the client with findings based on a balanced look at other weapon types, including nuclear, biological, chemical, radiological, and explosive threats. It was a pragmatic choice to balance the desire to converge on an exciting and relevant topic against the workshop's aims to explore multiple types of weapons. If certain threats were more prominent in our data, the analysis could run the risk of up- or down-playing certain types of threats at the risk of under- or over-investment in particular measures.

Divergent thinking taken to the extreme is not a panacea. Futurists usually are not interested in imagining every threat scenario and the effects a threat has on every person. Still, they are interested in the subset of most plausible threats in the timeframe being studied (usually over the next decade). More importantly, threatcasting is most useful as a structured starting point rather than as a complete inquiry into a specific threat. The purpose of divergent thinking is to discover multiple paths to move the trajectory of the future away from undesirable threats. Ideally, gatekeepers and decision-makers would then apply resources and take action early enough to avoid or mitigate a future disaster along as many paths as possible, however, every proposal has its priority and not all would be covered. Having to apply resources and plan for *every* contingent threat is paralyzing and not beneficial to any organization. It becomes very costly in currency,

bodies, and social capital to clean up after a future disaster, so wise practitioners tend to seek solutions that they can take action on rather than attempt to find a solution for every plausible threat.

The opposite of divergent thinking is, of course, convergent thinking. One would suppose that threatcasting favors divergent thinking over convergent thinking in all cases since divergence has the highest probability of casting a wide enough net to encompass those scenarios most likely to contain a novel finding. Up to a point, this supposition is true. That point is somewhere around Round Two: Finding Meaning in the post-analysis process when convergent thinking becomes more valuable. Here, there is a push-me, pull-you balancing act between convergence and divergence.

In the threatcasting framework, a futurist's work begins during pre-workshop analysis with a scan of the literature for guidance and advice on how one should structure the threatcasting foundation. Starting from a firm grasp of history, the threatcasting futurist must evaluate current events and expected social, political, and technological trends before springing into scenario development. Granted, there are multiple competing versions of history and each has its perspectives that shape the starting point from which a futurist understands the present. It is left to the futurist and their application of responsibility to decide what factors and what version of history is the starting point, including the client’s perspective of history. Regardless of how the analyst proceeds, the fact remains that an understanding of history and its various versions is necessary to comprehend the present and thus investigate how both shape the future.

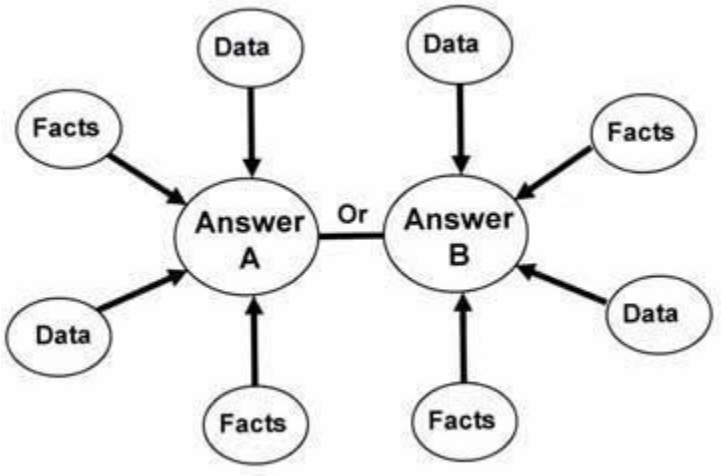
This analytical work continues with “in-stride analysis” during a workshop session. Monitoring the rate and quality of scenarios that workshop participants create is

critical to ensuring that later analysis has a strong base of data from which to begin post-analysis. Often, a returning participant who better understands the process can create a model that has more detail and answers the workbook prompts fully and with strong imagination. First-timers, on the other hand, may get caught up answering one or two prompts in depth and fails to respond to prompts, usually in the backcast. These models may lack details that would simplify comparison and aggregation of ideas between models.

In post-analysis, the futurist takes inputs from numerous places - pre-analysis research, subject matter expert opinions, raw data from the workshops, and current events - and distills these data into a few generalized findings. Figure 13 illustrates the idea of the convergence of multiple data sources into generalized findings at the end of post-analysis.

Figure 13

Convergent Thinking



Note. Licensed under Creative Commons Attribution-ShareAlike 3.0 (Msingh209, 2012).

Post-analysis, as I previously mentioned during the overview of threatcasting in Chapter 3, is the analytical phase in which the analyst summarizes the models, investigates the data for common themes - often through clustering and aggregation exercises - and ultimately relates the findings to the threatcasting foundation by making recommendations for action and awareness. Previously, I considered post-analysis as a process. In this chapter, I investigate post-analysis as an art. To do this, I first investigate the nature of novelty from the perspectives of psychology, biology, patent law, and journalism.

During this investigation, I illustrate how the imagination attribute becomes prominent in the futurist's thinking. Next, I connect the tradition and practices of intelligence analysis with the processes of post-analysis. This comparison reinforces the relationship between the attributes of analytics and imagination, but it is most helpful for the analyst to know when their analysis is complete. As the futurist applies a varying mix of analytics and imagination near the end of post-analysis, they should be able to find an answer to the question, "When do I feel I have found every reasonable conclusion supporting the requirements of the threatcasting foundation?" - or more simply put, "When am I done?"

These questions reflect the oscillating nature of convergent and divergent thinking. Methodical investigation of the data at hand first requires divergence to comprehend the thrust of the analysis, whereas understanding completion requires convergence and recognizing when coding, clustering, and thematic analysis all point to a few synthesized findings. And, sometimes, these generalized findings become the highly

desirable yet elusive evolutionary novelty. I use the attribute of imagination to categorize all the interpretations of novelty that follow.

The Nature of Novelty

During the final round of post-analysis, called "Finding Novelty," the analyst seeks to generalize the nature of a project's threats by creating several high-level findings to put into the final written report. This happens when all the analyst's data and processes converge on the generalized findings and the analyst wraps up their conclusions. These regular findings stay within the scope of the threatcasting foundation's research question and provide adequate responses to the foundation's application areas. There are plenty of guidance and action items for gatekeepers to consider in their follow-on planning sessions. Regular novelties often are simply "good enough" to meet the aims of the project, but they may not trigger a paradigm shift.

The idea of a paradigm shift is attributed to the writings of Thomas Kuhn. Kuhn, an American philosopher of science, wrote the famous book *The Structure of Scientific Revolutions* (1962) that suggested scientific discovery and scientific revolution happen in sudden shifts rather than in a steady or incremental way. These sudden shifts happen because the structures of theory, rules, and identity (e.g., the paradigm) within a field are not sufficient to compensate for discrepancies or anomalies within the framework defined by the field (Firinci Orman, 2016). For example, Aristotelian-era theories described nature in terms of natural states (i.e., an object falls to the ground because its natural state is there). Later, the natural sciences shifted toward Newtonian theories of motion that

discuss forces on objects (i.e. the force of gravity defines the action of an object falling to the ground) rather than describing motion in terms of natural state (Bishel, 2017).

When a profoundly different idea emerges, a new paradigm, with its inherent theory, rules, and identity is formed. Kuhn originally meant for paradigm shifts to describe scientific revolutions in thought, practice, and identity, but contemporary uses of the paradigm shift have made their way into macroeconomics (Keynes, 1936) software engineering (Ralph, 2018), and even to pop culture and marketing (Fulford, 1999). I am not advocating that a paradigm shift in the threatcasting sense conforms to the strict Kuhnian definition of a scientific revolution. Rather, I hope to link the idea of novelty with the spirit of distinct (and sometimes permanent) change that may happen when we observe patterns in the data suggesting to gatekeepers that their contemporary practices are not sufficient to deal with a future threat.

As I investigated the theories and practices of threatcasting post-analysis, I discovered there is yet another level of scrutiny the analyst could seek. I submit that a threatcasting report's ultimate goal is to identify if and when a profoundly new way to consider the future threats exists within the data. This is because ordinary findings do not make decision-makers sit up and pay attention. Decision-makers pay attention to "extra-ordinary" imaginings that suggest the future will be much more chaotic and troublesome than they initially thought unless they step up to do something to avoid the threat or mitigate its impacts. Occasionally, the future creeps up on us without much warning, and the best decision-makers can do is to help clean up the mess and recover from the event, even if that means understanding how the threat has permanently changed the status quo.

I call these infrequent findings that forever upset the status quo "evolutionary novelties." Often, the client chooses

Novelty, a word meaning new, unusual, or unique (*Novelty*, n.d.), sometimes seems so understood that its meaning is now trite, except in specific contexts, such as patent law, biology, psychology, journalism, and threatcasting. In psychology, a novelty is an experience that is often paradigm-shifting and one that causes a person to think differently or see the world in a new way. The most straightforward paradigm shift is an experiential novelty, or one that the analyst recognizes they and most others have never before seen or "personally experienced in their own lifetime" (Kanazawa, 2010). In my interviews with experienced threatcasting analysts, I confirmed that experiential novelty is a clear and decisive category for threatcasting futurists to filter and recognize a profound finding worthy of further investigation. Several participants described this experiential novelty as follows:

- "Something I haven't seen before in my corpus of knowledge" (Participant 2)
- "So there's any on any given day, there's probably, you know, out of a hundred things, if I think 50 of them are novel, the reality is that, almost all of those 50 somebody else has already experienced or encountered, or it's already a reality. I just haven't been exposed to it." (Participant 2)
- "All the signs say something is possible, but no one's talked about it yet" (Participant 4)
- "What's new about this that I've never thought about before or that we haven't seen before?" (Participant 4)

Each of the participants recognized that the first time they observed a new idea, it caused them to pause. In the talk-aloud tracks each participant recorded, I noticed that each person had a different way to register this moment. “Oh, wow!” one participant said. “Interesting…” was another typical response that more than one participant used. One simply grunted, “Huh…” before reflecting on what caused them to think about their observation in a new way. I spent considerable time trying to understand what parts of the scenario the participant was reading or thinking about just before the “pause” and attempted to ask more questions about that moment in the follow-on interviews. To a person, they all had to take a moment and re-read the transcript of the talk-aloud track before they realized they had made a pause. Most were not aware of what caused them to connect the new idea with an experiential novelty, but each participant confirmed that the “pause” was linked to an idea they wanted to explore further.

Further research is required to identify if the “pause” can be anticipated or made more apparent to the researcher so that they might reflect on the inputs more systematically. At a minimum, I believe that this moment is an opportunity to implement a memoing event, whether in the form of a journal, a researcher’s notebook, or even a brief entry in the post-analysis workbook. Recognizing when one uncovers an experiential novelty is the first step to becoming more aware of discovering the second category of novelty or the evolutionary novelty.

Biological and Psychological Novelty. The other, more complicated, paradigm shift is the concept of evolutionary novelty, or in a biological and psychological tradition, “entities and situations that did not exist in the ancestral environment” (Kanazawa, 2010). This definition was initially used to describe a hypothesis of how general intelligence

developed in humanity and is used in the field of developmental psychology. The field of evolutionary psychology also theorizes that psychological traits are evolutionary adaptations to requirements placed on cognitive stressors in the environment (Buss, 1995).

Evolutionary novelty is also a concept used in biological evolution, as scientists try to discover how new traits arise in organisms and facilitate permanent modification of the species. Biologists consider evolutionary novelty to be an adaptation of function (e.g., flight or vision) or an adaptation of structure (e.g., wings or eyes, respectively) (Nitecki, 1990; Pigliucci, 2008; Wagner & Lynch, 2010). The structure of wings is a necessary but insufficient condition for a species to achieve flight. Many species of birds have the proper structure (wings) but lack the function (flight). Either criterion works to describe the changes at a biological level, and we can use the function versus structure framework in our post-analysis toolkit. Assessing whether a novelty changes society's function or changes society’s structure is a fascinating way to frame deeper levels of data analysis, because this could potentially influence the suggestions a futurist gives to a client for action, depending on how the client wanted to respond to the threat. Functional and structural action items could look remarkably different. As I did not test whether a finding altered the structure or the nature of society, the application of this to threatcasting should be the subject of future research.

This idea of evolutionary, potentially irreversible change has tremendous importance to my theory that there is a difference between threatcasting’s novelty category and the emergence of certain special implications of unprecedented futures that decision-makers are not prepared to address. I found evidence of the evolutionary

paradigm shift in my discussions with experienced futurists. Participants never named evolutionary novelty, but these are some descriptions that suggest it exists in the minds of futurists:

- What we report on "may make people uncomfortable" (Participant 4)
- "Why will this thing add new value to the world? Because it's not just about synthesizing what people wrote, the output should add new value." (Participant 4)
- Novelty is "finding what isn't in the data" and imagining "the bigger things we aren't seeing" (Participant 2)
- "I still feel like it's going to matter and perhaps only to one reader who knows how it might be relevant" (Participant 5)
- This step is "creating a door instead of a mirror" (Participant 2)
- "It's like that moment where you realize the star you've been looking at, or the star that you didn't even notice, because it was just in the firmament, you know, you get to this point where you realize, 'Oh, that's the headlight of the train coming at us.' That's not, that's no star, that's [no] moon, that's a fully operational deathstar!" (Participant 2)

Participant 4 suggested that novelty should "add new value to the world." The type of value threatcasting seeks to offer are new ways to view threats that will improve our ability to meet them head-on. Sometimes, the value of the novelty is a reminder that the threat is likely to evolve in such-and-such a way. Other times, we may need to re-examine critical assumptions that precede our understanding of the world and make an evolutionary leap to a new paradigm. In *Two Days After Tuesday: A Science Fiction*

Prototype (Johnson & Winkelman, 2016), the evolutionary shift was the threat actor's manipulation of supply chains using innocuous home automation programs to flood the market with perishable goods and force repair parts to be deprioritized. From now on, planners must consider how seemingly unconnected supply chains (e.g., food supplies versus radiation detector repair parts) are inextricably linked due to automation and artificial intelligence. In *Information Warfare and the Future of Conflict* (Johnson et al., 2020), the idea of binary conflict (at war or at peace) was turned on its head with the introduction of quantum frameworks of conflict. We now must think of the implications (legal, social, and ethical) of being in both a state of war and a state of peace simultaneously. Finally, in *The Future of Extremism and Extremist Narratives in America* (Brown et al., 2021), we described the idea of normative extremism, and we submit that attacks against the norms and values that underlie the pursuit of the American dream should be evaluated in the same context as physical violence. Normative extremism also includes attacks using virtual violence through social media and "swatting," or deceiving emergency services to respond to a made-up threat. Each of these examples is an evolutionary shift in how we should think about future threats and add value to planning efforts across government and military organizations.

There are several other examples of novelty that support the idea of adding value to the world. In 2017, Johnson, Draudt, Vanatta, and West found that in the future, a company developing weaponized artificial intelligence software would be indistinguishable from a video game company developing AI for a new gaming platform (Johnson et al., 2017, p. 19). In another report on the future of weaponized narratives, researchers at the Threatcasting Lab found that information disorder machines (IDMs), as

a unique piece in the information warfare arena, are used only to pit "the worst of ourselves against ourselves" (Johnson, 2019, p. 30). A manifestation of pure manipulation, the IDM can get a person to "destabilize their values, and take actions that they normally would not" (p. 30). The ability of IDMs to target society at the individual level fundamentally changes the character of information warfare.

So, what makes these examples evolutionary and not just thought-provoking examples of what could happen a decade from now? In the first scenario on the AI weapons factory, few people would object to companies using AI to make a gaming platform better, more adaptive to players, or otherwise valuable for keeping players on the platform for more extended periods. Research and development to improve AI for games is a natural and expected progression of the field, and there is no cause for alarm. On the other hand, a growing number of organizations are protesting the use of AI for making autonomous and adaptive weapons. Autonomous weapons that do not have a human in the decision-making loop are rightfully a cause for apprehension, so it is appropriate to have concerned groups openly discuss the ethics of their use. The novelty arises when we realize that *right now,* there are no mechanisms to ensure that a gaming AI and an autonomous weapons AI are distinct types of innovation. Arguably, the processes to make them good pieces of software are nearly identical, yet applying the same processes has a drastically different end state.

The second example about IDMs suggests that novelty is uncovered not in the technology itself but in the highly complex ways that the idea is woven into society. In this case, IDMs are not a technology but a way to use automated discovery, personalized targeting, and individualized messaging to manipulate people on such a base cognitive

level that they do not recognize the manipulation. Gatekeepers seeking to minimize the effects of IDMs may find that there is no single thread to pull. Influence tactics occur in social media news feeds, advertising pop-ups, and on television. Any of these ways can pass along an individualized and weaponized message. Recognizing that the technology of IDMs has such a potentially disruptive effect on society is the evolutionary idea here.

Novelty in Patent Law. In U.S. patent law, "novelty" has a precise definition and one of three conditions an inventor must meet to receive a patent from the U.S. Patent and Trademark Office. A patentable invention must also be useful and non-obvious (*Novelty Patent: Everything You Need to Know*, n.d.; 35 U.S. Code § 102). For an idea to maintain its novelty status, it must:

1) "Not be shown to any third party, including friends and family.
2) Remain out of media, including journals, magazines, websites, etc.
3) Not be considered common knowledge to experts in the field.
4) Not have gone on sale prior to the patent filing.
5) Not have been built by a person that abandoned or concealed the idea." (*Novelty Patent: Everything You Need to Know*, n.d.)

There is a strict interpretation of novelty here that requires the inventor to prove that they are worthy of legal protections for their idea. Anytime the inventor makes a mistake by revealing an idea at the wrong time or to the wrong people, they may jeopardize the tenets of novelty and cost the inventor their patent.

Novelty in Journalism. In journalism, a reporter seeks to "scoop" a story and put it on the front page. In a 24-hour news cycle, a leading story could be on top of a social media feed. When deciding the newsworthiness of a story, journalists consider many factors such as impact or consequences, conflict, loss of life, degree of property damage, proximity, prominence, timeliness, human interest, or novelty (Rogers, 2019). In

describing novelty, Rogers (2019) uses an old journalism quip: "'When a dog bites a man, no one cares. When the man bites back—now that's a news story.' The idea is that any deviation from the normal course of events is novel and thus newsworthy." While this author relies on the generally accepted understanding of novelty (simply meaning something new), and since threatcasting is already in the business of finding the significant "deviations from the normal course of events," it appears that the journalistic understanding of novelty is not very helpful. This is not the case, as several key ideas from the journalistic view need closer examination.

There is a commonly understood relationship between humans and dogs. Humans are superior, the owner or master, and the dog should generally obey the master in all situations. The human provides shelter and food, and the dog provides companionship, entertainment, and protection. We also know that a dog has sharp teeth, and a dog with a vicious or unruly demeanor could be unsafe. We might discover a pattern of dog attacks during post-analysis and may even decipher underlying causes, but these would likely remain in the "Finding Meaning" column of our analysis. There isn't anything new or unprecedented about the threat of dog attacks in the future without some additional context or changes in environmental conditions over the next decade. Maybe that change is the accidental release of a virus that causes dementia and aggressiveness in dogs, in which case, the interesting finding is still not the threat of a dog attack but rather the source of how such a virus got loose. Perhaps the motivations of the threat actor would be something else to investigate. Following this line of inquiry would most likely provide us conclusions about the use of genetically modified viruses to record in our "Finding Novelty" column of post-analysis.

The second part of the journalism quip reads: “When the man bites back - now that’s a news story.” Using the same standard of evaluation in post-analysis, we might consider this interesting and worth examining for other patterns and underlying causes, not because it is new, but because it is rare and flips the tables on our usual understanding of the relationship between humans and dogs. It is quite conceivable for a person to bite a dog, and one can imagine any number of circumstances in which that would be only mildly interesting. But, to some analysts, this might be a case of experiential novelty, meaning one they haven’t seen before. If that were true they would likely spend some time considering the causes of a person biting a dog. Does the scenario contain any indication of social or technological changes that could cause this aberrant behavior? Are there multiple instances of human-biting-dog that indicate something else is at work? A pattern of humans biting dogs would first manifest in the “Finding Meaning” round of post-analysis. Depending on the other salient factors of newsworthiness, the analyst might again address the idea in the “Finding Novelty” round.

There are two other newsworthiness factors that I found much more important to our quest to filter evolutionary novelty from generic novelty. Those are *proximity* and *timeliness* of the threat. Proximity has both a geographic and a temporal dimension to it. The closer a threat is to the client’s geographical seat, the more compelling and motivational the threat might be. To be clear, in a hyper-connected world with near-instant communication, rarely is a geographical seat simply limited to a physical location. There are social geographies that pool people with similar interests and perspectives worldwide - this is the power of social media platforms. There are ethnic and racial geographies that ignore physical borders and link genealogical and national diasporas.

And there are even age geographies that some previous threatcasting reports have recognized.

The temporal dimension of proximity closely aligns with the attribute of timeliness. Timeliness suggests that some threats (or at least the precursor conditions to a threat) may appear sooner than others. This suggests that timeliness indicates a sense of urgency to the client who might prioritize certain recommendations for action ahead of others. This is also why, in the backcasting phase, we ask participants to put flags and gates into milestones approximately four years out and eight years out, allowing gatekeepers to plan for both short-term and long-term arrivals of any of the threat's indicators.

Another sense of timeliness is that of relevancy. Current events influenced both the projects on the future of WMDs and the investigation of extremism in America. The rising number of worldwide cases of COVID-19 strongly piqued the interest of workshop participants seeking to understand the near-term and long-term effects of a purposefully engineered or weaponized virus. As I pointed out earlier, the first round of models strongly reflected that emphasis, with eleven of the fifteen scenarios focusing on some type of weaponized virus. Likewise, during the extremism project, our analytical team lived through the violence and extremist activities at the Capitol Building during the 2021 Presidential transition of power. Although none of us were in Washington, D.C. during the events, we still needed to pause and consider how these current events affected our analysis and whether extremism a decade later, in 2031, would be noticeably different.

To elaborate on the idea of age geographies, I illustrate a couple of examples from *Digital Weapons of Mass Destabilization: The Future of Cyber and Weapons of Mass*

Destruction (Johnson, Brown, et al., 2021). During this workshop, several groups developed scenarios in which threat actors genetically engineered viruses and computer attacks to target elderly populations to cause the affected people to act in a non-typical way. Team Green Pawn 1 imagined a threat using a computer virus to compromise the digital pacemaker devices installed in elderly patients. The threat then coerced the victim to conduct random acts of violence else the computer virus would cause the pacemaker to fail, killing the victim. Team Mint Green Pawn 1 imagined the threat of a genetically modified virus that only affected the DNA of elderly victims, and the cure was held in "ransom" for those who could pay.

Recognizing Novelty Through Confirmation Bias. The final way futurists might recognize novelty comes through noticing when one is falling into the trap of confirmation bias. Participant 2 described how they recognized when an idea was novel, when they said it should "[create] a door instead of a mirror." Looking into a mirror typically returns the viewer's image in the reflection. This is a type of confirmation bias - one in which a person seeks information that justifies and supports their beliefs or opinions and rejects information that contradicts or provides alternative explanations. On the other hand, I believe the door is a metaphor for pushing aside confirmation bias and stepping through a threshold into a completely different environment. Participant 2 used the mirror or door framework to measure how much they felt an idea reflected their own beliefs or how much the idea felt like stepping through a doorway into a new environment.

Participant 4 also suggested that some novelties "may make people feel uncomfortable." Comfort here reflects a high degree of confirmation bias. It may also

reflect a high degree of homophily, or the idea that people who are similar (in thought, look, or background) tend to feel more comfortable around each other. The former is hazardous to solution-seeking as contradictory yet relevant information is often discarded. In contrast, the latter is dangerous to responsible design ideas and creating solutions that benefit marginalized groups rather than a select few. Making people feel uncomfortable is a strong indicator that the futurist has discovered something that might upset the status quo and thus be considered evolutionary.

Comparing Threatcasting and Intelligence Analysis

In the previous section, I illustrated the attribute of imagination by referencing various angles a futurist might consider to check for novelties in the data. In this final section, I tie together the attributes of analytics and imagination and investigate how they relate to the oscillatory nature of divergent and convergent thinking. This investigation relies on comparing post-analysis to intelligence analysis traditions and practices, which I lean on from my personal and professional experience while serving in the U.S. Army. Intelligence analysis is a style of analysis that aims to estimate what could reasonably happen in the future, primarily when focused on actions a threat actor would most likely take. I submit that intelligence analysis celebrates the analytical response of converging on the *best* answer given current information.

Heuer (1999) suggests a checklist of six steps in the analytical process that should improve the process of intelligence analysis: 1) defining the problem, 2) generating hypotheses, 3) collecting information, 4) evaluating hypotheses, 5) selecting the most

likely hypothesis and 6) ongoing monitoring of new information (p. 173). Heuer provides this list of actions as one remedy to avoid analytical errors, mostly centered on not recognizing different types of bias and their effect upon both the analyst and the analytical process. As a meta-framework, these six steps are already present in the threatcasting process and suggest a cycle that oscillates between divergent and convergent thinking dependent upon the step.

Step one: defining the problem – convergent thinking. The threatcasting foundation defines the project's scope and creates a working boundary that includes a narrowed topic, a research question, and an application area. This allows futurists working on the project to set aside questions or observations that, for the time being, fall outside the threatcasting foundation. However, outliers that are discovered during the remainder of the process may require renegotiation of the foundation.

Step two: generating hypotheses – divergent thinking. In normal circumstances, the threatcasting foundation does not *explicitly* suggest any hypotheses that might answer the research question or application areas. In the case study of extremism in America (see Chapter 5), we generated a hypothesis about the nature of the relationship between identity, the narratives that support identity, and an actor's motivations to move to extremist behavior. While threatcasting futurists do generally not practice this approach, the case study demonstrates that a hypothesis-driven method is viable and testable with the threatcasting framework. Similarly, there is an unwritten and *implicit* hypothesis that becomes apparent during Phase Zero activities and the development of threatcasting foundation. Deciding which subject matter experts might provide the right kind of input or inviting participants with valuable experience or the proper position to implement

effective change is at its core a hypothesis. This hypothesis suggests that only a specific combination of facts, trends, people, and recommendations for action can best understand and imagine the future and then avoid, mitigate, or recover from threats. In generating multiple hypotheses, the analyst practices divergent thinking, but then may trim away some hypotheses that are not testable under a given framework or with available data.

Step three: collecting information – divergent thinking. I have already demonstrated that the Phase Zero activities of selecting the right experts, participants, and prompts are essential to generating the right amount of information about the future. The other necessary information is a large amount of background research and fact-checking that analysts do during Phase Four (post-analysis and report writing) to tie models of the future to trends and fact-check findings with experts.

Step four: evaluating hypotheses – divergent & convergent thinking, and *Step five: selecting the most likely hypothesis – convergent thinking*. Evaluating and selecting hypotheses is the essence of Phase Four (post-analysis). The three-step Summary-Meaning-Novelty process seeks to identify trends between models that describe and illustrate what decision-makers should be watching for and how to manage the time until the future threat appears. The three-step process also identifies outliers that do not cleanly fit within the trends but are interesting (or dangerous) enough to be highlighted and considered separately. As analysts consider how codes congregate as clusters or how clusters rise to higher-level themes, they are essentially evaluating whether the data confirms or refutes a hypothesis and seeking the right way to describe the trends they observe in the data. Once this "right way" to describe the data becomes apparent, it becomes a finding that the analyst describes and validates in the report writing step.

Finally, *Step six: monitoring for new information – divergent thinking*. At the end of Phase Four (report writing), the threatcasting process requires analysts to ensure their findings are grounded in reality, meaning the trends are plausible and possible in the next decade. Additional research, fact-checking, interviews with experts and practitioners, and reflection on assumptions and biases provide a more robust set of findings. Threatcasting also suggests opening the findings up for peer review during this phase. Here, peers are generally the subject matter experts and participants who initially contributed to the data modeling process. Peer review is done to ensure the findings are plausible and possible and that recommendations for action are taken seriously.

For example, while writing our findings on the future of extremism, my analytical team was suddenly bombarded with new information when the presidential transition of power and the storming of Capitol Hill occurred. This caused the team to momentarily pause and reflect on whether an ongoing extremist incident would have any immediate effect on their findings. As we collected news reports and early assessments of extremist ideologies found among some of the events, we reassessed our hypothesis about the relationship between identity and radicalization risk (see Chapter 6). It turned out that the event validated two of our three key findings concerning algorithmic amplification and corporate extremism but caused us to update the language and assessment on normative extremism that wasn't as visible from the modeled data.

Despite being sound advice for improving analysis, this step-wise checklist lacks a discussion on how to know when the analysis is complete. How does a futurist know when to stop evaluating new information, updating hypotheses, and testing new theories? More importantly, how does one know when a mundane finding is, in fact, an

evolutionary novel discovery that could fundamentally change how we see the problem in the first place? Imagination, in the sense that the analyst needs to understand when to broaden their views and take in more information or tightly focus on one aspect of the data or another, is coupled with the attribute of analytics to demonstrate that threatcasting has both procedural and exploratory qualities.

When to Stop?

One of the most challenging moments in post-analysis is knowing when the analysis is complete, and the findings are the best available given the data and inputs. My observations suggest that when an analyst thinks they are nearing the end of their work, they consider three things. The first is their process, the second is how the results will be communicated to all the various stakeholders, and the third is whether their findings are responsible. I will discuss the first two considerations here and address responsibility in depth in Chapter 7.

As the analyst reviews their processes, they should review any memos they wrote and possibly re-code the memos for one last pass of insights. Other procedural reviews could be mentally reviewing whether the analyst was faithful to the three-round post-analysis process or did they move freely between summarizing, finding meaning, and finding novelty. Are there items of interpretation in the summary column that should have been included in the finding meaning column instead? Does that change the output at all? If the analyst used computer software to aid in qualitative analysis, are there any new functions or tools within the software that can provide one more look at the data?

For example, when I used Dedoose to manage my codes and excerpts, I was able to generate code co-occurrence matrices that provided another layer of analysis. Figures 9 and 10 found in Chapter 5 illustrate these matrices and offered a visual representation of when specific codes were found in proximity to other codes, suggesting a relationship between them. This type of visualization is cumbersome and prone to errors if not done in software.

Next, the analyst should consider and prepare for final report writing. The most critical output from a threatcasting project is communicating the results to several different audiences simultaneously (government policymakers, developers in industry, academic researchers, military strategists, and the general public). This is a fundamental difference between threatcasting and other foresight methods. Whereas many foresight methods attempt to narrowly meet the needs of organizational strategies (i.e., maximizing profits, seeking new investments, or improving product placement), threatcasting outputs are more often than not suitable for a wide variety of audiences. As futurists, we attempt to help the reader answer the implicit question, "Why should I pay attention to this threat?" The ultimate goal is to encourage readers to answer for themselves, "What is my part in avoiding, mitigating, or preparing to recover from this threat?" Imagining how a reader from the government might interpret the data versus how a post-doctoral researcher at a university might interpret the data should suggest to the analyst any gaps in their work. While the primary audience (usually the client) should be the main focus for preparing the communication plan, the savvy analyst should seek the nuances that provide information for adjacent audiences to see the problem in a valuable light.

The analyst should also consider focusing strategies to "prioritize the multiple observations and reflect on their essential meanings" (Saldaña, 2016, p. 274). Saldaña (2016) suggests four strategies for focusing on the essential findings of a project. First is the "top 10" list. Physically print out the ten most crucial documents from the project and lay them out in various arrangements. These documents can be extracts from a model, an analytical memo, an excerpt from a subject matter expert transcript, or any personal correspondence with the client or other analyst. He suggests that the documents could be organized "chronologically, logically, hierarchically, telescopically, episodically, narratively, from the expository to the climactic, from the mundane to the insightful, from the smallest detail to the bigger picture, etc." (p. 275). Since each study is unique, several combinations might provide new insight.

The second focusing strategy is one that I prefer to use. I seek to isolate and name the study's "trinity." A trinity restricts the analyst to considering only the study's three most important concepts arranged in a Venn diagram. Suppose the study has findings with recognizable degrees of magnitude, such as global, local, and individual. In that case, the three Venn circles might be the macro-level or most significant finding that applies globally. The meso-level sits in the middle, and the micro-level could focus on an individual or a single organization (Saldaña, 2016, p. 275).

The third focusing strategy, called codeweaving, is already inherent in the post-analysis process. This technique takes keywords and phrases and weaves them into a narrative. Saldaña (2016) submits that the exercise might seem artificial at first. Still, he suggests using it as "a heuristic to explore the possible and plausible interaction and interplay of your major codes" (p. 276). In many ways, the spreadsheet method that

Professor Johnson teaches by recording summary, meaning, and novelty in separate columns already meets the intent of codeweaving. However, I suggest the analyst expands the exercise one step further by creating a short, written narrative in complete sentences to test whether the codes make sense when put together in new ways. As it currently stands, the spreadsheet method tends towards bullet points and brief phrases rather than a purposeful narration of the findings.

The final focusing strategy is perhaps one of the most abstract. Saldaña (2016) calls this the "touch test." He suggests that higher-level generalizations should be concepts that one cannot touch. "You can touch an old house in poor disrepair, but you cannot touch the phenomenon of 'poverty.' And you can touch a painting an artist has rendered, but you cannot physically touch the artist's 'creative process'" (p. 276). The analyst should review their high-level findings and test them for touch. If the concept seems too tangible, consider higher-level phenomena and concepts that describe the finding's essence more accurately.

Only when the analyst has taken the time to reflect on their processes, reviews their findings through one or more focusing strategies, and considers the implications of responsibility can they honestly say to themselves, "I am finished with post-analysis." The next chapter provides the analyst an in-depth look at the final piece of this puzzle. I submit that strategies of responsible innovation, design theory, and risk governance are the minimum frameworks necessary to invoke the final attribute of thinking-like-a-futurist to ensure that a threatcasting project addresses future change and avoids "future shock."

CHAPTER 7

DESIGNING THE FUTURE RESPONSIBLY

In the introduction of this research, I referenced the idea of future shock or the "shattering stress and disorientation that we induce in individuals by subjecting them to too much change in too short a time" (Toffler, 1970, p. 19). Adapting to the shock of change by engineering, designing, and deliberately preparing for the future is precisely the remedy, but does humanity have the tolerance, the tools, or the *time* to ensure the future is "better" for everyone or only for a select few?

In this chapter, I deliberate the third leg of the thinking-like-a-futurist triad—responsibility—and argue that a futurist must consider various positions of what a "better" or "successful" future means and for whom (the tolerance). I investigate several perspectives of responsibility, including traditions of future design, technology innovation, and socially responsible innovation. These perspectives allow us to consider how actions today ripple into future changes (the tools).

I am purposefully vague about a definition of "design" as the mechanics, principles, and frameworks taught by design schools and business schools are not my bailiwick. However, my academic and professional training put me in a unique position to consider and reflect on the impacts of a product, process, technology, or even policy decision. I consider a "designer" to be a person in a position to make purposeful decisions about their or someone else's future. Design, then, includes resource allocation, understanding the timing of subsequent decisions, and knowing how to assess the effects of their decisions.

Tolerance

Making the world better is a hallmark of design principles. The non-profit design studio IDEO takes an optimistic approach to the future and believes humans can control the future shock through human-centered design.

> "Embracing human-centered design means believing that all problems, even the seemingly intractable ones like poverty, gender equality, and clean water, are solvable. Moreover, it means believing that the people who face those problems every day are the ones who hold the key to their answer" (IDEO.org, 2015, p. 9).

In this context, IDEO is primarily concerned with the design of "things" like products, but they also focus on the design of services, experiences, and social enterprises. We must consider both tangible products and intangible services or processes as equal outcomes of a responsible innovation approach.

When researching an innovative product or process, designers should consider how the outcome appeals to society's normative targets (von Schomberg, 2013). For the European Union, these normative targets come from Article 3 of the Treaty on the EU. European social norms include the promotion of scientific and technological advance, ensuring a competitive social market economy, promotion of social justice, equality between women and men, solidarity, and the fundamental rights of human beings, sustainable development, and quality of life - including a high level of protection for human health and the environment (European Union, 2010 as listed in von Schomberg, 2013, p. 57 and figure 3.2 p. 58).

In contrast, the United States roots its political and social norms in the Declaration of Independence and the achievement of "life, liberty, and the pursuit of happiness." Unfortunately, few substantive documents in the U.S. are widely accepted as promoting

any long-term normative targets. However, designers, entrepreneurs, and policymakers in the U.S. can lean on rich scholarship about *values* to justify their pursuit of responsible innovation (a discussion of RI follows in the next section).

Schwartz (2010) identified 19 universal basic values that regulate how people both "express personal interests and characteristics" and how people "relate socially to others" (p. 227) (see also S. H. Schwartz, 2012; S. H. Schwartz et al., 2012). These values form a continuum, best visualized on a wheel rather than a straight line that transitions between self-enhancement and self-transcendence and back again. In an idealized world, it is the latter category of values in the realm of thinking beyond one's self, namely universalism, benevolence, tradition, conformity, and security, that make up the bulk of socially normative values that best reflect the aims of architects of a "better future." It is when these architects (or designers, entrepreneurs, etc.) favor the values of power, achievement, hedonism, stimulation, and self-direction without considering the socially normative ones that we see power imbalances arise and the stifling of marginalized voices as the victims such as in previous eras of innovation.

Unfortunately, the world is not idealized and power imbalances can occur in situations where intentions are good. The following section on tools provides several frameworks for designers to judge whether their designs are more closely aligned with personal (self-enhancement) or social (self-transcendent) values – and whether these values achieve desired end states. These frameworks illustrate some steps to ensure broader inclusivity and sensitivity to the interconnectedness of innovative technologies and processes.

The concept of tolerance requires a warning about the dangers of irresponsible innovation, or those attempts to design the future by “practices where stakeholders were unaware of the importance of the innovation’s societal context” (von Schomberg, 2013, p. 60). These practices include four types: 1) technology push, 2) neglect of fundamental ethical principles, 3) policy pull and 4) lack of precautionary measures. Stilgoe, Owen, & Macnaghten observe that “while actors may not individually be irresponsible people, it is the often complex and coupled systems of science and innovation that create what Ulrich Beck (2000) calls ‘organised irresponsibility’” (Stilgoe et al., 2013, p. 1569).

Briefly, *technology push* is when a corporation introduces new technology and considers some long-term effects, such as safety, but is not sensitive to cultural differences or opinions from opposing viewpoints. It is like a corporation saying, "You want this, but don't know it yet."

Von Schomberg (2013) described the push of genetically modified soybeans in the mid-1990s as a case study. Monsanto, a company that had been developing genetically modified food for years, introduced modified soya into European markets without allowing the European Union sufficient time to study or consider their product's social implications. Even though GM food might have long-term social benefits such as hunger prevention or drought resistance, non-governmental organizations rapidly mobilized and pushed for reactive bans. The public grew increasingly distrustful of Monsanto’s tactics, and soon all GMOs were lumped into the same category, regardless of their value to society. Von Schomberg states,

> "This example shows how substantial dissent among major stakeholders can frustrate responsible technological development. NGOs felt that they had little influence on the direction in which this technology would lead us. Regulations

> were exclusively focused on safety aspects, and the broader environmental, social, and agricultural contexts were not brought into the equation" (p. 61).

Social media platforms might also be considered a manifestation of technology push. When Facebook initially launched in 2004, only a few envisioned its long-term effects on society, both for self-enhancement and self-transcendence. David Kirkpatrick, the author of *The Facebook Effect*, shares an early assessment of the platform's reach when he wrote,

> "Facebook is bringing the world together. It has become an overarching common cultural experience for people worldwide, especially young people. It changes how people communicate and interact, how marketers sell products, how governments reach out to citizens, even how companies operate. It is altering the character of political activism, and in some countries it is starting to affect the processes of democracy itself. This is no longer just a plaything for college students" (Kirkpatrick, 2010, p. 15).

Over a decade after Kirkpatrick's book, Facebook has grown even more prominent and more influential over much of the world's social media exposure. In 2021, Facebook is facing continued scrutiny by the U.S. Congress for its role in tolerating an environment in which groups use the platform to coordinate civil disobedience, promote extremist ideologies, and manipulate public opinion through misinformation during the 2020 presidential election (Leskin, 2021).

Neglecting ethical principles might occur when personal interests conflict with public values. An example of conflicting ethical principles is an innovation for speedier health care that does not adequately protect personal data privacy. *Policy pull* happens when technologies are used for political purposes, sometimes beyond their intended uses. The rush for full-body scanners at airports followed several security incidents and policymakers were eager to show that "something was being done" without considering

privacy and technology limitations (von Schomberg, 2013). Finally, the *lack of precautionary measures* often stems from "decision making under scientific uncertainty and scientific ignorance" (von Schomberg, 2013, p. 63). Despite policymakers' best efforts to surround themselves with the best science available, there are times when science doesn't have a suitable answer, or may never be capable of producing one, but a decision still needs to be made.

Tools

Earlier, I mentioned that unavoidable and constant change is one of the most powerful forces of human existence. Yet change is not intrinsically undesirable. Another of the most potent forces unique to humanity is the capacity to *design*. Bruce Mau describes design as

> "one of the world's most powerful forces. It has placed us at the beginning of a new, unprecedented period of human possibility. It encompasses the utopian and dystopian possibilities of this world, in which even nature is no longer outside the reach of our manipulation" (as quoted in Carrott & Johnson, 2013, p. 333).

To some, the idea that we would even consider manipulating nature reflects the hubris of humanity. To others, it reflects the boundless imagination that only humankind has achieved (whether through evolution or divine grace) that sets us apart from mere animals. Design thinking tools allow all people to consider their current circumstances and imagine whether there is something more or better (or even worse or different) waiting for them tomorrow or the day after tomorrow. Using these tools requires

responsibility and accountability, as each choice today is inextricably linked to another person and *their* choices.

The three most powerful tools that have demonstrated the most impact on future design from the perspective of a threatcasting futurist are the concepts of responsible research and innovation, adversarial design, and risk governance. Let's take each of these in turn.

Responsible Research and Innovation

Responsible research and innovation (RRI) is a bundled term used within European academic and political circles and has some weight as a legal, or at least an institutionally normative, standard within the European Union. It comprises the ideas of "responsibility," "innovation," "responsible research," and "responsible innovation," each of which has a subtly different meaning. RRI is foremost a social innovation. By convention,

> "Responsible Research and Innovation is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)" (von Schomberg, 2013, p. 63).

RRI is also a framework to discuss the pros and cons of the "division of moral labour" in which scientists discharge their "moral obligation to work towards progress." In contrast, others "look after social, ethical, and political issues" (Rip, 2014). Von Schomberg (2013) argues that RRI looks at both the product (the technologies, devices, and artifacts of social progress) and the processes of innovating. The RRI view of

responsibility, another form of moral obligation, is for the "consequences of implementation... primarily related to the properties and characteristics of the products or the technology and less to the privileged owners and creators of the technology" (von Schomberg, 2013, p. 53). This means that producers of products and processes should consider their design's social consequences and not just rely on that design's economic success to show how responsible the innovation is.

One definition of innovation is "improvements of existing products and services...being achieved via the free market" with the "normative dimension of what counts as 'improvement' … decided by market mechanisms" (von Schomberg, 2013, p. 54). However, innovation needs to be broader than merely improving a product's impacts in economic markets. It should respond to the societal Grand Challenges of "global warming, tightening supplies of energy, water and food, ageing societies, public health, pandemics, and security" (Lund Declaration, 2009, as quoted in von Schomberg, 2013, p. 58).

A variant to RRI is the U.S. concept of responsible innovation (RI). "Responsible innovation means taking care of the future through collective stewardship of science and innovation in the present" and includes the four dimensions of anticipation, reflexivity, inclusion, and responsiveness (Stilgoe et al., 2013, p. 1570, also Table 2, p. 1573). For RI to be effective, these four dimensions should be integrated and embedded in the development of product design and its implementation (Stilgoe et al., 2013, p. 1573).

While RI as a concept calls out the collective social element of innovation, it does not explicitly tie the end state of innovation to normative goals, grand challenges, or other types of social good like RRI does. Implicitly, Stilgoe, Owen & Macnaghten argue for a

requirement for the “capacity to change shape or direction in response to stakeholder and public values and changing circumstances” (2013, p. 1572, under heading “responsiveness”). Still, the U.S. generally lacks a clear social end state and instead tends to let market forces fuel innovation.

Adversarial Design

The second tool we can use to improve social tolerance and avoid future shock is understanding adversarial design. According to DiSalvo (2012), “...through designerly means and forms, adversarial design evokes and engages political issues. Adversarial design is a type of political design” (p. 2). It is a close cousin to critical design (Malpass, 2012) and tactical or experiential media (Shedroff, 2001). This relationship with politics means “...these artifacts and systems are adversarial because they represent and enact the political conditions of contemporary society and function as contestational objects that challenge and offer alternatives to dominant practices and agendas” (DiSalvo, 2012, p. 115).

An object designed with the intent of bringing to light a political schism allows us “something literally to point at with regard to the political condition: they can be manifestations - expressive encapsulations - of some aspect of the political condition” (DiSalvo, 2012, p. 117). One example is the *Million Dollar Blocks* design project by Laura Kurgan that maps crime data to answer the question “Where does the prison population come from?” rather than the common question “Where does crime occur?” (DiSalvo, 2012, p. 8). This project challenges normative views of crime and urban

planning and seeks to illuminate the geographies of prison populations instead of geographies of crime.

The main thrust of adversarial design is to constantly challenge and confront the status quo, dissent with the "way we always do things," and ensure that democratic politics cannot rest in a state of lazy majority without questioning the beliefs and practices of those in power. Its purpose is to highlight cultural and political blindness towards the status quo that does not consider other ways of doing things that might not marginalize certain groups repeatedly. Adversarial design thus provides a way to "critique" policy, politics, and processes.

Adversarial design also calls on the philosophy of *agonism* or a particular political perspective that illustrates the conflict and contestation that is a hallmark of democratic politics (DiSalvo, 2012). "Agonism is a condition of forever looping contestation. The ongoing disagreement and confrontation are not detrimental to the endeavor of democracy but are productive of the democratic condition," suggests DiSalvo (2012, p. 5). Agonism as a philosophy isn't just about "sticking it to the man" but has a solid potential to form red teams that find flaws in one's risk assessment about the future.

What is persuasive about adversarial design is the concept of "adversary." Rather than making the contest between enemies "that seek to destroy one another," adversary here characterizes "a relationship that includes disagreement and strife but that lacks a violent desire to abolish the other" (DiSalvo, 2012, p. 6). In essence, it's a contest between the "relations and experiences aroused through the designed thing and the way it expresses dissensus" (DiSalvo, 2012, p. 7). The primary purpose of this adversarial struggle is to draw attention to ways of knowing that promote biased, gendered,

historical, or narrow-minded ways of preparing for the future and instead ask, “who is being left out, and how do we include them?”

In this sense of seeking who is being left out, adversarial design is a close cousin to threatcasting post-analysis processes. One of the questions we as futurists always ask ourselves during post-analysis is, “Who is missing?” or, said differently, “What are we not talking about?” Often, this is an indicator that we have recognized bias in the design of our scenarios or our analytical processes. Contemplating any missing perspectives necessitates a tremendous increase in the imagination attribute. It requires the analyst to consider whether the data gap is from a failure of the inputs or whether it indicates the existence of an evolutionary novelty that the analyst has yet to grasp. Returning to the data and soliciting the aid of others to share their insights on the data is an effective way to know whether the missing conversation is a data gap or an analytical oversight.

Risk Governance

The final tool to help humans lessen the shock from impending future change is the idea of risk governance, which blends control, coupling, communication, and culture into an agile process that actively considers how innovation affects the future and reacts accordingly. Using a risk mindset offers the perspective that innovation is “a process of generating new knowledge, ideas, and inventions, and translating these into concepts, products or processes that protect this value” (Maynard, 2015, p. 731). It opposes the linear process of risk identification, assessment, and mitigation (Maynard et al., 2012, p. 169) against profits or technology development. It expands beyond assessing the hazards

to human health and the environment by considering how "local technology innovation is highly dependent on global factors" (p. 173). In other words, risk governance attempts to draw in global threads of social change when trying to assess the impact of technology on "the full panoply of personal, social, environmental, technological, economic, political and corporate risks" (Maynard, 2015b). In this sense, risk governance can also be applied to process innovation and cultural shifts, rather than just to new products.

Each tenet of risk governance (control, coupling, communication, and culture) is opposed by natural forces resistant to change that may increase the risks of innovation. These oppositional forces include fear, uncertainty, speed of change, entrepreneurship success, or fiscal responsibility to shareholders. As outlined by the International Risk Governance Council (IRGC) and Maynard, Grobe, & Renn (2012), an examination of the Risk Governance Framework guides entrepreneurs, policymakers, and the lay population on using risk as a way to anticipate and design a better future.

Control - As science improves to allow us more precise control over nanotech and the biological building blocks of technology (e.g., synbio), we can anticipate a reduction in specific hazards to human health and the environment and the increase of others. Engineered biothreats, for example, may bypass current controls such as detection and immunization. According to the IRGC, hazards differ from risks in that hazards "describe the potential for harm or other consequences of interest" (IRGC, 2005, p. 19). They characterize the "*inherent properties of the risk agent and related processes*" while risk describes "the *potential effects that these hazards are likely to cause*" (Ibid., emphasis in original). Better control over the technical properties of materials may reduce environmental exposure and reduce hazards. However, the product's technical control is

not the end of responsibility. Developers must also consider what society may think about these new products, how a product is accountable to society, or how a product might be used for purposes outside the designer's intent. For instance, the introduction of advanced nanotech and synbio products may lead to emerging challenges such as supply chain management or exploitation of raw material extraction as new materials, processes, and products are being discovered. One oppositional force to finer control is generalized fear and "concerns over scientists 'playing God'" (Maynard et al., 2012, p. 170).

Coupling - One of the dangers of unconstrained innovation is forgetting that "humanity's actions are intimately coupled to environmental re-actions" (Maynard et al., 2012, p. 170). The IRGC categorizes this intimate coupling of causal links as *complexity* -- invoking all the good baggage that complexity theory brings to this discussion, which I will not further elaborate here (IRGC, 2005, p. 29). The speed of information transfer, the growth of intertwined global markets, and globalized politics sensitivities have steadily increased in this, the fourth industrial revolution (Schwab, 2016).

Over the past half-dozen generations, there has been a non-linear acceleration of coupled changes, with impacts harder to predict and more resistant to control. Was there any way for the designers of ARPANET, the precursor to the modern Internet, to have foreseen how Russia could fundamentally disrupt the nature of American democratic elections in 2016 through a campaign of false and misleading information on social media networks with global implications towards the future of privacy and democratic processes? Hardly. Contrast this with loosely coupled systems (of which there are arguably fewer and fewer) affecting change at the local level, and perturbations in the systems are often damped by surrounding communities (Maynard & Garbee, 2019).

Communication - Scientific to "lay" populace communication via open-access and electronic publications is flattening previously held "intellectual and decision-making hierarchies" (Maynard et al., 2012, p. 171) with new opportunities for unconstrained action. With the non-linear growth of innovation, there has also been an evolution of ideas, not constrained by geography, on the debate and best practices of how science should be done. This debate is now global and increasingly decentralized. Fortunately, this international debate empowers groups previously without a voice but is opposed by uncertainties of power concentration and the "trustworthiness of sources and manipulation of data" (p. 172). This means that scientific and academic communities are being called upon to ensure that the voiceless and marginalized are part of the ongoing discussion on innovation. Without them, future hazards and risks of innovation will undoubtedly continue to marginalize and discount minority voices.

Culture - Lastly, risk governance argues for a cultural shift from entrepreneurs and corporations. To minimize, mitigate, or recover from perceived (and actual) hazards of innovation, corporations must be accountable for the *results* of products and processes rather than just their safe (and profitable) design. These results must consider social changes and broader impacts that extend farther than profit margin and market share. Maynard (2015a) wants us to look beyond the external boundaries that RI appears to set on entrepreneurs and instead build it into the very processes of entrepreneurship. Luckily, this ties us closely to the frameworks of RRI and RI, described earlier. In particular, the dimensions of anticipation and responsiveness play strongly in shaping the culture of being accountable for the results of products and processes (Maynard & Garbee, 2019; Stilgoe et al., 2013). Corporations should "move towards values-based business models

that are increasingly responsive to stakeholders - including citizens" (Maynard et al., 2012, p. 173). This cultural shift is strongly opposed by economic forces and the need to get products to market with its corresponding fiscal responsibility to shareholders.

Insights

One thing about measuring the benefit of the future, or rather, measuring whether a product is going to have the positive impact we assume it will have, is that we will never see all the ramifications of our actions. Yet, when our future becomes their history, our children will judge us for failing to predict the fall-out from our decisions. The outdated way of allowing a few influential people, corporations, or governments to make sweeping decisions for the rest of society is shifting. As tools such as design thinking, responsible research and innovation, risk governance, and event threatcasting become further available to practitioners, more individuals may be given the power to push against the natural tide of history and affect future change.

We can only forecast a few of the outcomes of innovation, regardless of how much responsibility we pour into our efforts, because of how interconnected and complex everything is. Sometimes, ripple effects are relatively predictable and may even be desirable to set into motion something that should appear in the future. However, those ripple effects can only be expected to appear in a brief amount of time down the road - the farther away we look, the less sure the results of our choices today will manifest in expected ways tomorrow. Therefore, we should take an extra measure of caution when

invoking solutions if we don't fully understand how our actions are linked to complex systems.

This extra measure of caution also applies to the recommendations and suggestions we, as futurists, provide in threatcasting reports. It is far easier to recognize and recommend solutions during the backcast that are comfortable for the client to implement, but these are not always "responsible." For instance, during the separate backcasting session conducted at the Naval Postgraduate School investigating the future of information warfare, several participants recommended solutions that conformed to *current* applications of U.S. military doctrine. They were not engaging imagination and responsibility to consider *future* changes to doctrine that might be more successful for information warfare goals in the future. One of the recommendations to counter adversarial uses of information was for the military to develop the ability to "insert an American narrative into any system, at any time" (Johnson et al., 2020, p.46). As an analytical solution, this recommendation made sense; as a responsible solution, it missed the mark. Our response was to challenge the assumptions behind the recommendation and illustrate where the Department of Defense could look to modify these assumptions.

> "This belief relies on the principles of democratic theory, meaning that the US/ western way of life should be superior to other ways of life because we have a democratic governance model. Additionally, if we want to be able to 'insert our narratives' into another cultural system, it will not be in English and will need to be culturally nuanced and savvy for how those in the system receive narratives. This exposes an overwhelming challenge the Department of Defense (DoD) faces in recruiting multilingual and multicultural savvy recruits from a national base composed primarily of a population that collectively undervalues these skills" (Johnson et al., 2020, p.46).

Using tools that invoke thoughtful processes about the future, we can ensure that humanity's hubris in designing our destiny is present only when we discard responsibility.

The best available approach to limiting negative effects in the future is when we take a cue from the European framework of responsible research and innovation (RRI), couple that with critical and adversarial ways of designing products and processes, and finally govern those designs with a risk-focused framework. Entrepreneurs, corporations, policymakers, and researchers all have an obligation to make the design of the future more inclusive of historically marginalized voices; to design products and processes that achieve values-based outcomes, such as equity, justice, quality of life, and sustainable development; and to include those whose lives are affected every day by the problems our designs aim to solve. Only with thoughtful, purposeful, and responsible frameworks of design, inclusion, and risk management can we avoid the paralyzing effects of stepping into a future, unable to act or make decisions that are for the benefit of the 801st lifetime of humanity.

CHAPTER 8

CONCLUSION

Limitations and Uncertainties

This research has some limitations, including the small sample size of futurists trained in threatcasting and the personalized nature of experiences. The backgrounds each futurist uses as the lens to examine the raw data of future scenarios is not homogenous. The goal isn't to robotize or clone analysts to arrive at the same conclusions. In fact, threatcasting is such a suitable tool because it embraces diverse and even ridiculous thinking to imagine the worst the world can throw at us. Novel conclusions provide decision-makers *now* as much time and space as possible to avoid surprises ten years down the road.

There is also a limitation in the number of case studies I am conducting to show evidence for varied ways to do data analysis. Since each threatcasting project has different aims, depending on the client's needs, and given that qualitative research is highly dependent on the raw data available to study, it is not always possible to choose the best methodology for data analysis at the beginning of a project. On the one hand, letting the data guide and define the findings in a grounded theory approach is nearly always appropriate. On the other hand, I offer that sometimes it may be appropriate to test the data against a preexisting theory, which may be particularly useful when revisiting or validating an existing strategy. I am investigating a singular test case using a hypothesis-driven approach, and in doing so, acknowledge that I may come to

inconclusive results about this method. Additional research would help solidify the cases in which a hypothesis-driven approach would be more appropriate.

Another limitation of my research is that it includes an autoethnography in a personal narrative voice that describes my experiences and growth as a threatcasting analyst. This does not mean that my experiences are valueless. In fact, autoethnography argues that personal experiences are essential to a complete view of society, and augmenting empirical research with personal views makes for arguably more effective science. Ellis & Bochner (2000) state, "The truth is that we can never capture experience...but if representation is your goal, it's best to have as many sources and levels of story recorded at different times as possible. Even so, realize that every story is partial and situational" (p. 750).

I also claim that there is a framework for studying and improving the art of the analyst that others might benefit from. However, this framework may only help me; others who attempt to follow the methods I describe may have limited success in finding evolutionary novelty in the way I explain. So, I submit that this research does not contain a thorough analysis of the art of the analyst; however, my contribution to this topic will further the scholarship of threatcasting.

I am confident that a systematic review and investigation of how other analysts at the Threatcasting Lab think through data to reach conclusions and findings will also contribute to the scholarship of threatcasting. More importantly, I will become a better researcher and analyst by listening to and reflecting on the stories that the other analysts tell about their own experiences. In the same vein, I sincerely hope that other analysts will open themselves up to my findings so that we may move toward "a spirit of

collaboration, understanding, and openness to experience and participation" (Ellis & Bochner, 2000, p. 760). It is this shared experience - a shared *human* experience - that makes threatcasting such a valuable tool for studying the future.

There is also uncertainty in how exactly I can measure one technique's added value compared to others. There is simply no way to test whether *in vivo* coding, process coding, hypothesis coding, or any other technique helps a researcher draw closer to the elusive "novelty" than another one could. In any qualitative study, the key is to become intimately familiar with the data and then code or parse it over and over again from many different angles (Saldaña, 2016). There is also no way to test whether any of these approaches are inappropriate for threatcasting and should be categorically removed from the analyst's repertoire; there are simply not enough futurists trained in any formal methodology to understand this. So, for now, I will claim that the analytical methodologies I illuminate and personally use will do nothing but improve the art and craft of the threatcasting analyst.

Finally, understanding what could be novel is as much art as it is science. This research attempts to bring a few more credible and familiar analytical tools into the toolbox so that the creativity and "art" of making sense of tomorrow's threats are as well-informed as possible. The art and science of threatcasting analysis is a very new field of study. I hope to contribute some structure to the process so those who follow may spend more time understanding the threats they are trying to study than worrying about the methods of how to get there.

Future Research

There are four areas of future research identified in this study that are outside the immediate scope of this dissertation. Three directly investigate additional insights of the threatcasting process. The fourth is a topic of current events and was generated during the analysis of data on the future of extremism in America.

The first topic is assessing novelty by testing changes in societal function against changes in societal structure. This mirrors the idea of novelty from a biological evolution paradigm. The assessment of novelty in this manner would likely be categorical rather than some other evaluation that one novelty was better or worse than another. Hypothetically, I could imagine a researcher incorporating frameworks of social structure such as definitions of family units, the span of government influence (e.g., local, state, or federal), or geographical proximity to health care. These could then be contrasted with frameworks of social function such as the value of nurturing, the impact of taxes for educational purposes, or assessing peer influence on personal fitness, respectively.

Another topic for future research is investigating how the backgrounds of workshop participants affect the types of futures developed. I have demonstrated that the curation of participants and experts during Phase Zero sets the tone for a threatcasting project, because these are the people who directly contribute to the models we assess in post-analysis. Changing the composition of attendees would likely change the tone and style of models, all other things being equal. But understanding how much the data changes would necessitate several controlled experiments investigating the same topic but with different groups of participants. Detailed interviews with participants would be

necessary to isolate variables such as political views, historical perspectives on specific topics, education levels, experience in applying responsible design methodologies, and general demographics. Differences and similarities in test groups might help answer the question, "Who is being left out?" and may provide insight into data gaps or analytical trends that threatcasting is inadvertently pointing towards.

The third area of investigation that could be addressed is additional testing of the hypothesis-driven approach. This study demonstrated a single case using frameworks of narrative identity and radicalization risk to assess whether there was a relationship between identity and extremism. Our conclusions were based on the data available, the frameworks we used, our interpretation and application of those frameworks, and the experiences and background of the analysts involved. Those are a lot of variables to consider and testing each one separately would be problematic. The simplest step along this path would be to conduct additional projects using the hypothesis-driven approach and compare and contrast multiple cases for similarities, differences, regular appearances of bias, and other factors. This could indicate whether an inductive approach or a hypothesis-driven approach is more appropriate for some types of projects rather than others.

Finally, the last area of future research is topical. During the post-analysis of our project on the future of extremism in America, Renny Gleeson and I discovered occurrences of events that did not directly use violence and thus were not "extreme" according to definitions from the FBI, were probably legal, but were clearly attacking values and norms. We coined the term "normative extremism" to describe actions and activities that attempted to undermine the relationship between formal laws and societal

stability. We intend to continue to study normative extremism in other contexts and to publish additional research on the topic.

What I Learned

To end, I would like to reflect on some of the lessons I have learned during my investigation of threatcasting. I have learned about threatcasting itself, mainly about the post-analysis process, and I have learned about myself. What follows are the major lessons I hope to share with other futurists.

Lessons about Threatcasting Processes

1. The data aren't the answer, but they are a catalyst - a springboard - that forces us to think about the future in ways that are not obvious. In threatcasting, good data comes from a well-designed workshop during the substantial effort given to Phase Zero activities. Pre-analysis, thoughtful curation, and a helpful steering committee are essential to success in Phase Zero.
2. Backcasting needs more attention to get right. Workshop participants are usually more focused on the imaginative side of developing a scenario that they neglect imagining the solutions. Training people to think about responsibility is one way to ensure better gates, flags, and milestones make it into the model. Setting aside a separate event to focus only on backcasting inputs is another way.
3. The client is the first gatekeeper. One of the futurists I interviewed is a business person who assists companies in strategic design. They are heavily focused on

practical recommendations the client can do, so they focus on the client as the primary gate holder. In their interview, this person said, “if I'm doing this for a client, I better put gates in there that my client can own because that doesn't make sense. Otherwise, like I'm giving them recommendations for what they need to do. They better be able to own those gates. Everything else is a flag so they can observe it” (Participant 4). This perspective may be helpful in improving the quality of backcasting during a workshop with inexperienced participants or with a time constraint by focusing backcasting on gates, flags, and milestones that are relevant to the primary client. This takes some practice from workshop facilitators to recognize and to implement in their sessions.

4. Reusing data (models) is acceptable and useful. I demonstrated one case study in which we used models from previous workshops to understand future conditions and trends. Although we specifically filtered the repository of available scenarios that the Threatcasting Lab has published for markers necessary to complete our analysis of extremism, we recognized they could be used for much more than that. These scenarios provided varying perspectives of future social, economic, political, and technological conditions that would be useful to a wide variety of future threats. As threatcasting grows, a formalized repository of scenarios would only improve the types of futures we could envision and the interconnectedness of them all.
5. Round One: Summarizing. In simplest terms, summarizing is useful to understand the intent of the model only. Participant 2 stated that the step of summarizing should be, “an honoring of the thing that they have created. And that's really in

the summary – that it is being as true to what you can determine is the spirit of their argument using the facts." In terms of analytical processes, separating the intent of the model's creators from one's personal interpretation is a matter of discipline and practice. It is quite easy, and I found myself doing it regularly, to trivialize understanding the intent of the model before moving on. Doing so may lead to missed insights.

6. Round Two: Finding Meaning. This is the step in which the analyst should begin interpretation of the model and seeking early implications. Disciplined and thorough coding using multiple coding styles is one way to structure the various ways the futurist might interpret these implications.
7. Round Three: Finding Novelty. Generalizing and synthesizing codes, themes, categories, and interpretations of them into high-level findings that cut across all (or most) of the models is the intent of this step. While this is the last round of post-analysis, it is not the end of analysis as the futurist still needs to tie these findings to the threatcasting foundation by answering, "Do these findings answer the research question?" and "What suggestions for action do these findings make for the client?" Occasionally, Round Three conclusions become a catalyst for a new round of considering the implications of experiential and evolutionary novelty.

Lessons about Foresight in General

1. People matter. Those invited to work on a project will shape inputs and outputs. The analysts who bridge the gap between data (as a catalyst for thinking) and the client's goals (project objective) will fundamentally affect the project's output.
2. The thinking-like-a-futurist triad is one way to describe how the analyst guides the art of thinking: one part analytics, one part imagination, and one part responsibility. Each of these attributes has a more significant part to play during different stages of post-analysis. It is a way that works for me and may not work for others.
3. Data aren't the endstate. Modeling threat futures creates a data point, but none of these models will ever be exactly how the future turns out. What is important about data is how it helps us discover new ways of thinking about the future and where our blind spots are.
4. Minimize the "shock" of the future. The purpose of foresight is not to predict the future. Rather, it is to provide evidence that other perspectives of the future exist. Systematically thinking about alternatives in some ways prepares the mind to accept oncoming change, prepare for it, and mitigate the shock and paralysis of unexpected surprise.

Lessons about Analytics

1. Use multiple coding methods, but not at the same time. Each pass through of the data, especially during the heavy coding that occurs in Round Two: Finding Meaning, should be done with a purpose. Structural codes differ from process

codes and each provides a different perspective of the data. Choosing an appropriate coding style is a factor of experience and the needs of the project.

2. "Memoing" is essential. At several points of the post-analysis process, the futurist should pause to write down moments of inspiration and to reflect on what dots were just connected to make a conclusion. Some suggesting memoing points include after each data pass through, when changing coding techniques, and anytime one "pauses" or says "interesting." The former records processes and is useful for validating techniques between analysts; the latter records moments when the brain is trying to connect the dots and may indicate moments of bias, learning, or new avenues of analysis.
3. Software-aided analysis is necessary for certain types of projects, especially those with testable frameworks and hypotheses. Computer-assisted qualitative data analysis (CAQDAS) is almost mandatory if testing a hypothesis driven approach or using multiple frameworks simultaneously. CAQDAS can also help organize large-scale projects, automatically filter for desired perspectives, provide visually-based reports and charts, or interface with quantitative and mixed-method approaches.
4. Processes are guidelines but not a substitute for critically evaluating change. Becoming proficient at the science of analysis is only part of the formula; be open to ambiguity, other ways of looking at data, and recognize you won't have all the answers. Lean on other people to strengthen you where you are weakest.

Lessons about Imagination

1. Finding novelty is full of imagination – as much art as science. Consider a moment during analysis that caused you to pause or reflect deeply on something. This could be a phrase in the data, a relationship between two codes, or the influence of current events. Is what you are seeing new because you have never experienced it? Can you find external evidence of that happening elsewhere? Or is what you are seeing a fundamental change in how the client may need to view the world in order to appropriately avoid, mitigate, or recover from a future threat?
2. Recognizing the difference between experiential novelty and evolutionary novelty is the key to understanding when a finding is "just right" or is instead paradigm-shifting. Keep asking, "What is missing? What are we not thinking about?" to see if a novelty exists but is simply escaping the attention of the analyst or if the data really have nothing new to reveal.
3. Outliers exist, but not all are important. Occasionally, there are pieces within models that don't collect into nice groupings and clusters. Are these outliers the result of the wild curiosity of the model's authors? Are they mildly interesting? Or are you missing something important? Consider using a different coding technique or consult a colleague to see if an outlier can be explained in any other context relevant to your work.
4. Be aware of the ridiculous: you might be missing something. Dator's so-called "Second Law of the Future" suggests that "Any useful statement about the future should at first appear to be ridiculous" (Candy, 2010, p. 202). Ridiculousness here might indicate an experiential novelty that warrants further investigation. Later,

ridiculousness may turn into learning or some realization of underlying assumptions.

5. Not every project has an evolutionary novelty; that's okay.
6. Balance between divergent and convergent thinking. Reflecting on one's thoughts is a meta-exercise in critical thinking and is not always easy. Understanding when one should seek additional inputs or when one should drill down into a narrow perspective is part of the art of analysis. Divergence often invokes a greater focus on imagination, whereas convergence leans more heavily on analytical processes.
7. Use focusing strategies to narrow Round Three conclusions. Round Three is when the analyst must synthesize all the codes, themes, categories, and insights from previous rounds of analysis. Often, synthesizing to a higher-level of understanding is chaotic and overwhelming and requires a great deal of imagination to see patterns. If conclusions are not readily apparent, the analyst may wish to implement a "Top 10," "Trinity," or "Codeweaving" technique (Saldaña, 2016). to help focus towards a smaller set of findings.
8. Reporting on the uncomfortable. In most circumstances, threatcasting relies on the data to tell a coherent story about specific categories of threats. On occasion, an analyst may discover something about the story that contradicts the aims and aspirations of the client and other gatekeepers. Something uncomfortable may indicate an evolutionary novelty that could upset the status quo. It takes courage to report honestly on what the data say, but it also takes courage to continually look at the dark sides of the future and remain optimistic.

Lessons about Responsibility

1. Be a "skeptimist" - a skeptical optimist. Threatcasting imagines the world at its worst and can easily make one believe that only the worst can happen. A healthy dose of skepticism helps us realize that many of the models we work with are simply science fiction with an element of truth. It is up to us as futurists to provide a vision of how to avoid the threats we study so that, in the end, we can achieve futures that are better for everyone.
2. Become a student of responsibility. The outputs we create as futurists may seem relevant for the client's understanding of the future, but what about those who have no voice in our models? How can we include ideas of equity, justice, and sustainability in the recommendations for action? Find appropriate ways to identify action items that include marginalized groups and non-governmental organizations with connections to them.

Threatcasting has the ability to peer a short way into the darkness of the future. At first glance, what we glimpse might shock us and might leave us paralyzed to take actions. But I submit that the tools, processes, and lenses I presented in this study will allow us to design paths that steer us away from threats and towards more hopeful futures. Indeed, as I began with words from the Tofflers, so I end with them.

> "These pages will have served their purpose if, in some measure, they help create the consciousness needed for man to undertake the control of change, the guidance of his evolution. For, by making imaginative use of change to channel change, we can not only spare ourselves the trauma of future shock, we can reach out and humanize distant tomorrows" (Toffler, 1970, p. 430).

REFERENCES

Alexander, A. (2016). Cruel intentions: Female jihadists in America. In *Program on Extremism*. George Washington University.

Aishwarya.gudadhe. (2015). *Divergent thinking*. Wikimedia. https://commons.wikimedia.org/wiki/File:Final_divergent_thinking.jpg

Benigni, M. C., Joseph, K., & Carley, K. M. (2017). Online extremism and the communities that sustain it: Detecting the ISIS supporting community on Twitter. *PLoS ONE*, *12*(12), 1–23. https://doi.org/10.1371/journal.pone.0181405

Bennett, M., & Johnson, B. D. (2016). *Dark future precedents: Science fiction, futurism and law* (Vol. 1, Issue September).

Bishel, D. (2017). *A contemporary assessment of Thomas Kuhn: The detection of gravitational waves as a Kuhnian revolution [Thesis, California State University Stanislaus]*. *July*, 5–12.

Bishop, P., Hines, A., & Collins, T. (2007). The current state of scenario development: An overview of techniques. *Foresight*, *9*(1), 5–25. https://doi.org/10.1108/14636680710727516

Brown, A. J. C., Gleeson, R., & Massad, J. (2021). *The future of extremism and extremist narratives in America*. Arizona State University.

Buss, D. M. (1995). Evolutionary psychology: A new paradigm for psychological science. *Psychological Inquiry*, *6*(1), 1–30. https://doi.org/10.1207/s15327965pli0601_1

Candy, S. (2010). *The futures of everyday life : Politics and the design of experiential scenarios. [Doctoral dissertation, University of Hawai'i at Manoa]*. https://doi.org/10.13140/RG.2.1.1840.0248

Carrott, J. H., & Johnson, B. D. (2013). *Vintage tomorrows*. Maker Media, Inc.

Charmaz, K. (2000). Grounded theory: objectivist and constructivist methods. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd ed., pp. 509–535). Sage Publications, Inc.

Cole, A., & Singer, P. W. (2020). Thinking the unthinkable with useful fiction. *Journal of Future Conflict*, *Fall*(2), 1–13.

Corbin, J., & Strauss, A. (2012). Criteria for evaluation procedures for developing grounded theory. In *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory* (pp. 297–312). https://doi.org/https://dx.doi.org/10.4135/9781452230153

Corman, S. R. (2016). The narrative rationality of violent extremism. *Social Science Quarterly*, *97*(1), 9–18. https://doi.org/10.1111/ssqu.12248

Crossett, C., & Spitaletta, J. A. (2010). *Radicalization: relevant psychological and sociological concepts*. Asymmetric Warfare Group.

Dawson, J. (2018, March 21). Relationships with God and community as critical nodes in center of gravity analysis. *The Strategy Bridge*.

Dawson, J., & Weinberg, D. B. (2020). These honored dead: Sacrifice narratives in the NRA's American Rifleman Magazine. *American Journal of Cultural Sociology*. https://doi.org/10.1057/s41290-020-00114-x

Department of Defense. (2012). *Handling dissident and protest activities among members of the Armed Forces* (1325.06; Department of Defense Instruction). https://doi.org/10.1093/milmed/148.11.857

Department of Defense. (2017). *Joint planning: Joint publication 5-0*.

Department of Homeland Security. (2019). *Strategic framework for countering terrorism and target violence* (Issue September).

DiFranza, A. (2021, February 17). *Predictive analytics: What it is & why it's important*. http://www.sas.com/en_us/insights/analytics/predictive-analytics.html

DiSalvo, C. (2012). *Adversarial design (Design thinking, design theory)*. MIT Press.

Dreborg, K. H. (1996). Essence of backcasting. *Futures*, *28*(9), 813–828. https://doi.org/10.1016/S0016-3287(96)00044-4

Ellis, C., & Bochner, A. P. (2000). Autoethnography, personal narrative, reflexivity: Researcher as subject. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of qualitative research* (2nd Ed., pp. 733–768). Sage Publications, Inc.

Fine, G. A. (1999). John Brown's body: Elites, heroic embodiment, and the legitimation of political violence. *Social Problems*, *46*(2), 225–249. https://doi.org/10.2307/3097254

Firinci Orman, T. (2016). "Paradigm" as a central concept in Thomas Kuhn's thought. *International Journal of Humanities and Social Science*, *6*(10), 47–52.

Fulford, R. (1999, June 5). Paradigm. *Globe and Mail*, 1–3.

Hardwig, J. (1985). Epistemic dependence. *The Journal of Philosophy*, *82*(7), 335. https://doi.org/10.2307/2026523

Hauck, J. (2020, September 4). Assessing the impact of defining lone actor terrorism in

the U. S. *Divergent Options*, 1–7.

Helmer, O. (1967). *Analysis of the future: The Delphi method*. The RAND Corporation.

Heuer, Jr., R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence. https://doi.org/10.3906/elk-1401-272

Hines, A., & Bishop, P. C. (2013). Framework foresight: Exploring futures the Houston way. *Futures*, *51*, 31–49. https://doi.org/10.1016/j.futures.2013.05.002

Hunt, L. (2013, October 17). Beware the lone wolf radicals. *Policemag*. https://doi.org/10.1016/s0262-4079(11)62149-0

IDEO.org. (2015). *The field guide to human-centered design*. Creative Commons 3.0.

IRGC. (2005). *Risk governance: Towards an integrative approach*. https://doi.org/10.1093/acrefore/9780190228613.013.246

Johnson, B. D. (2016). *A widening attack plain*.

Johnson, B. D. (2019). *Information disorder machines: Weaponizing narrative and the future of the United States of America*. Arizona State University.

Johnson, B. D. (2020, July 22). A lost generation of athletes. *Global Sport Matters*.

Johnson, B. D. (2021). *The future you*. HarperCollins Publishers.

Johnson, B. D., Brown, J. C., & Massad, J. (2021). *Digital weapons of mass destabilization: The future of cyber and weapons of mass destruction*. Arizona State University.

Johnson, B. D., Draudt, A., Brown, J. C., & Ross, R. J. (2020). *Information warfare and the future of conflict: A Threatcasting Lab report*. Arizona State University.

Johnson, B. D., Draudt, A., Vanatta, N., & West, J. R. (2017). *The new dogs of war: The future of weaponized artificial intelligence*. Arizona State University.

Johnson, B. D., & Vanatta, N. (2018). The inside enemy: Weaponisation of your logistical footprint. *Journal of Supply Chain Management, Logistics and Procurement*, *1*(1), 1–9.

Johnson, B. D., Vanatta, N., & Coon, C. (2021). *Threatcasting*. Morgan and Claypool Publishers.

Johnson, B. D., & Winkelman, S. (2016). *Two days after Tuesday: A science fiction prototype*. Cisco Hyper Innovation Living Labs.

Johnson, B. D., Winkelman, S., & Buccellato, S. (2018). *Engineering a traitor*. Army

Cyber Institute at West Point.

Johnson, B. D., Winkelman, S., Buccellato, S., & Badower, J. (2018). *Hero*.

Johnson, B. D., Winkelman, S., Burchielli, R., Hudson, D., & Haley, M. (2018). *11.25.2027*.

Johnson, B. D., Winkelman, S., Hudson, D., & Loh, K. (2018). *Silent ruin*. Army Cyber Institute at West Point.

Jones, S. G. (2018). The rise of far-right extremism in the United States. *Center for Strategic and International Studies (CSIS), November*, 9.

Kahn, H., & Wiener, A. (1967). *The year 2000: A framework for speculation on the next thirty-three years*. Macmillan.

Kanazawa, S. (2010). *What does "novelty" mean?* Psychology Today. https://www.psychologytoday.com/us/blog/the-scientific-fundamentalist/201006/what-does-novelty-mean

Keynes, J. M. (1936). *The general theory of employment, interest and money*. Macmillan Cambridge University Press.

Kirkpatrick, D. (2010). *The Facebook effect: The inside story of the company that is connecting the world*. Simon & Schuster, Inc.

Kuhn, T. S. (1962). *The structure of scientific revolutions*. University of Chicago Press.

Leskin, P. (2021, March 22). Facebook says it removed more than 1.3 billion fake accounts in the months surrounding the 2020 election. *Business Insider*.

Linstone, H. A., & Turoff, M. (1975). *The Delphi method : techniques and applications*. Reading, Mass. : Addison-Wesley Pub. Co., Advanced Book Program.

Linstone, H. A., & Turoff, M. (2011). Delphi: A brief look backward and forward. *Technological Forecasting and Social Change, 78*(9), 1712–1719. https://doi.org/10.1016/j.techfore.2010.09.011

Maan, A. (2015). *Counter-terrorism: Narrative strategies*. University Press of America, Inc.

Malpass, M. (2012). *Contextualising critical design: Towards a taxonomy of critical practice in product design [Dissertation]* (Issue September). Nottingham Trent University.

Marcus, G., & Davis, E. (2019, September 6). How to build artificial intelligence we can trust. *The New York Times*.

Maynard, A. D. (2015a). The (nano) entrepreneur's dilemma. *Nature Nanotechnology*, *10*(3), 199–200. https://doi.org/10.1038/nnano.2015.35

Maynard, A. D. (2015b). Why we need risk innovation. *Nature Nanotechnology, 10*(9), 730–731. https://doi.org/10.1038/nnano.2015.196

Maynard, A. D., & Garbee, E. (2019). Responsible innovation in a culture of entrepreneurship: A US perspective. In R. von Schomberg & J. Hankins (Eds.), *International Handbook on Responsible Innovation: A Global Resource* (pp. 488–502). Edward Elgar Publishing.

Maynard, A. D., Grobe, A., & Renn, O. (2012). Responsible innovation, global governance, and emerging technologies. In R. A. Parker & R. P. Appelbaum (Eds.), *Can Emerging Technologies Make a Difference in Development: Seeds of Science* (pp. 168–187). Tayler & Francis Group.

McAdams, D. P., & McLean, K. C. (2013). Narrative identity. *Current Directions in Psychological Science*, *22*(3), 233–238. https://doi.org/10.1177/0963721413475622

Menzies Foundation. (2020). *Regional Cyber Futures Initiative: The future of risk, security and the law*.

Msingh209. (2012). *Map of convergent thinking*. Wikipedia. https://en.wikipedia.org/wiki/File:Map_of_Convergent_Thinking.jpg

Nitecki, M. H. (Ed.). (1990). *Evolutionary innovations*. University of Chicago Press.

Novelty. (n.d.). Merriam-Webster's Online Dictionary. Retrieved March 25, 2021, from https://www.merriam-webster.com/dictionary/novelty

Novelty patent: Everything you need to know. (n.d.). Upcounsel.Com. Retrieved March 23, 2021, from https://www.upcounsel.com/novelty-patent

Oden Institute for Computational Engineering & Sciences. (2021). *Predictive data science*. https://www.oden.utexas.edu/research/predictive-data-science/

Pigliucci, M. (2008). What, if anything, is an evolutionary novelty? *Philosophy of Science*, *75*(5), 887–898. https://doi.org/10.1086/594532

Polletta, F. (1998a). Contending stories: Narrative in social movements. *Qualitative Sociology*, *21*(4), 419–446. https://doi.org/10.1023/A:1023332410633

Polletta, F. (1998b). "It was like a fever. . ." narrative and identity in social protest. *Social Problems*, *45*(2), 137–159. https://doi.org/10.2307/3097241

Polletta, F., Chen, P. C. B., Gardner, B. G., & Motes, A. (2011). The sociology of storytelling. *Annual Review of Sociology*, *37*, 109–130.

https://doi.org/10.1146/annurev-soc-081309-150106

Popper, R. (2008). How are foresight methods selected? *Foresight*, *10*(6), 62–89. https://doi.org/10.1108/14636680810918586

Quist, J., & Vergragt, P. (2006). Past and future of backcasting: The shift to stakeholder participation and a proposal for a methodological framework. *Futures*, *38*(9), 1027–1045. https://doi.org/10.1016/j.futures.2006.02.010

Ralph, P. (2018). The two paradigms of software development research. *Science of Computer Programming*, *156*, 68–89. https://doi.org/https://doi.org/10.1016/j.scico.2018.01.002

Rip, A. (2014). The past and future of RRI. *Life Sciences, Society and Policy*, 1–23. https://doi.org/10.1080/13869790701305921

Robinson, J. (2003). Future subjunctive: Backcasting as social learning. *Futures*, *35*(8), 839–856. https://doi.org/10.1016/S0016-3287(03)00039-9

Robinson, J. B. (1990). Futures under glass: A recipe for people who hate to predict. *Futures*, *22*(8), 820–842. https://doi.org/10.1016/0016-3287(90)90018-D

Robinson, W. S. (1951). The logical structure of analytic induction. *American Sociological Review*, *16*(6), 812–818. https://doi.org/10.4135/9780857024367.d13

Rogers, T. (2019). *What makes a story newsworthy*. ThoughtCo. https://doi.org/10.1163/9789087907358_003

Rowe, G., & Wright, G. (1999). The Delphi technique as a forecasting tool: issues and analysis. *International Journal of Forecasting*, *15*(4), 353–375. https://doi.org/10.1016/S0169-2070(99)00018-7

Saldaña, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Sage Publications Ltd.

Schuurman, B., Lindekilde, L., Malthaner, S., O'Connor, F., Gill, P., & Bouhana, N. (2019). End of the lone wolf: The typology that should not have been. *Studies in Conflict and Terrorism*, *42*(8), 771–778. https://doi.org/10.1080/1057610X.2017.1419554

Schwab, K. (2016). *The fourth industrial revolution*. World Economic Forum.

Schwartz, P. (1991). *The art of the long view*. Doubleday.

Schwartz, S. H. (2010). Basic values: How they motivate and inhibit prosocial behavior. *Prosocial Motives, Emotions, and Behavior: The Better Angels of Our Nature.*, *January 2010*, 221–241. https://doi.org/10.1037/12061-012

Schwartz, S. H. (2012). An overview of the Schwartz theory of basic values. *Online Readings in Psychology and Culture*, *2*(1), 1–20. https://doi.org/10.9707/2307-0919.1116

Schwartz, S. H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J. E., Demirutku, K., Dirilen-Gumus, O., & Konty, M. (2012). Refining the theory of basic individual values. *Journal of Personality and Social Psychology*, *103*(4), 663–688. https://doi.org/10.1037/a0029393

Shedroff, N. (2001). *Experience design 1*. New Riders Publishing.

Smelser, N. J., & Baltes, P. B. (Eds.). (2001). Analytic induction. In *International Encyclopedia of the Social and Behavioral Sciences* (Vol. 11). Elsevier.

Smith, A. G. (2018). *How radicalization to terrorism occurs in the United States: What research sponsored by the National Institute of Justice tells us* (NCJ 250171).

SocioCultural Research Consultants. (2020). *Dedoose* (Version 8.3.35).

Stilgoe, J., Owen, R., & Macnaghten, P. (2013). Developing a framework for responsible innovation. *Research Policy*. https://doi.org/10.1016/j.respol.2013.05.008

Taleb, N. N. (2009). *The black swan*. Random House.

Toffler, A. (1970). *Future shock*. Random House, Inc.

United States Air Force Academy. (2016). *Project on advanced systems and concepts for countering weapons of mass destruction (PASCC)* (USAFA-PASCC-BAA-2016).

University of Houston. (2020). *What is foresight*. https://www.houstonforesight.org/what-is-foresight/

Vanatta, N., & Johnson, B. D. (2019). Threatcasting: a framework and process to model future operating environments. *Journal of Defense Modeling and Simulation*, *16*(1), 79–88. https://doi.org/10.1177/1548512918806385

von Schomberg, R. (2013). A vision of responsible research and innovation. In R. Owen, J. Bessant, & M. Heintz (Eds.), *Responsible Innovation* (pp. 51–74). John Wiley & Sons, Ltd.

Wagner, G. P., & Lynch, V. J. (2010). Evolutionary novelties. *Current Biology*, *20*(2), 48–52. https://doi.org/10.1016/j.cub.2009.11.010

World Health Organization. (2020, January 5). *Pneumonia of unknown cause - China*.

Znaniecki, F. (1934). *The method of sociology*. Farrar and Rinehart.

APPENDIX A

THE RADICALIZATION RISK FRAMEWORK

The Radicalization Risk Framework

Code #	Risk Factor	Definition
1	**Emotional Vulnerability**	A strong emotional attachment to something or someone that is disrupted or changed, e.g., family love, patriotism, loyalty, etc. Rarely seen alone without other risk factors
2	**Dissatisfaction w/ Status Quo**	A sense that how things are now are not what the person wishes them to be
3	**Personal connection to grievance**	Personally wronged in the past; could be perceived or actual and perpetrated by an individual or that state
4	**In-group delegitimization of out-group**	Being excluded from the in-group or a feeling of not belonging or "fitting in"
5	**Non-negative view of violence**	Violence as a solution is acceptable through acculturation by media
6	**Historical views on violence**	Violence as a solution is acceptable from personal experience (I see it all the time, or I've used it before)
7	**Perceived benefit of violence**	Violence has been seen to be successful in solving problems (as a last resort or for a specific purpose)
8	**External support**	Support for violence comes from a benefactor (a nation-state or a corporation) - does not usually include money or materiel
9	**Resources**	Availability of sufficient capital and materiel means to enact violent actions
10	**Social net**	The network of social ties needed to draw someone over the fence towards violence
11	**Perceived threat**	There is a sense of danger to life, liberty, or the pursuit of happiness
12	**Extended conflict**	The animosities between groups or drive to violent solutions are not new and might be culturally and historically engrained

13	**Humiliation**	A specific type of grievance when a person is removed from their position of status or the actions of others cause personal embarrassment; may also be a motivator for nation-states
14	**Competition**	Usually, international competition between states (military, economic, etc.); an individual loyal to the state may adopt their state's drive to be on top as a personal narrative
15	**Youth**	Younger individuals (teens & early adults) may be more likely to be drawn to violent solutions
16	**Resonant narrative**	For our purposes, not used since this is the variable we are seeking to discover

Note. The radicalization framework contains sixteen risk factors observed across various studies of radicalization and counter-radical applications. Adapted from Crossett & Spitaletta (2010).

APPENDIX B

THE NARRATIVE IDENTITY FRAMEWORK

The Narrative Identity Framework

Identity Construct	**Definition**
Agency (A)	"The degree to which protagonists are able to affect change in their own lives or influence others in their environment, often through demonstrations of self-mastery, empowerment, achievement, or status. Highly agentic stories privilege accomplishment and the ability to control one's fate."
Coherent Positive Resolution (CPR)	"The extent to which the tensions in the story are resolved to produce closure and a positive ending."
Redemption (R)	"Scenes in which a demonstrably "bad" or emotionally negative event or circumstance leads to a demonstrably 'good' or emotionally positive outcome. The initial negative state is 'redeemed' or salvaged by the good."
Contamination (Con)	"Scenes in which a good or positive event turns dramatically bad or negative, such that the negative affect overwhelms, destroys, or erases the effects of the preceding positivity."
Exploratory Narrative Processing (E)	"The extent of self-exploration as expressed in the story. High scores suggest deep exploration or the development of a richly elaborated self-understanding."

Communion (Comm)	"The degree to which protagonists demonstrate or experience interpersonal connection through love, friendship, dialogue, or connection to a broad collective. The story emphasizes intimacy, caring, and belongingness."
Meaning Making (M)	"The degree to which the protagonist learns something or gleans a message from an event. Coding ranges from no meaning (low score) to learning a concrete lesson (moderate score) to gaining a deep insight about life (high score)."

Note. The narrative identity framework includes seven constructs theorizing how people create meaning about their lives. Adapted from McAdams & McLean (2013).

APPENDIX C

INTERVIEWS WITH FUTURISTS - QUESTIONS

These interview questions were used in the follow-on interview with futurists trained in the threatcasting methodology. The first group of general questions was given to each person. In contrast, the specific questions were generated after reviewing the participant's "think aloud" video they submitted on their assessment of the same three scenarios. The intent was to capture each participant's train of thought and how they moved from raw data to conclusions and identify whether they recognized if an evolutionary novel finding existed within the data. Many of the questions were generated on the fly during the interview and, as such, have not necessarily been edited for grammar, spelling, or punctuation. The names are the participants are withheld for privacy purposes.

General Interview Questions

- In a sentence or two, would you please describe your background?
- What "label" most closely describes your work with the future? (some ideas: futurist, futurologist, foresight practitioner, threatcasting practitioner, foresighteer, researcher, consultant, global futures strategist, strategic planner, etc.)
- What traits are most desirable as a threatcasting practitioner/futurist? (some ideas: analysis, creativity, responsibility, global perspective, trends research, etc.)
- When do you know you are transitioning from summarizing, to finding meaning, to finding novelty? What distinguishes the transition boundaries?
- What is the difference between a strong model and a weak model?
- If there is no story in the model, how would you suggest improving it?

- What percentage of analytics, imagination, responsibility is in each round (summary, meaning, novelty)?

Specific Questions for Participant 1

- What does "interesting" indicate for you? (line 47, 50, 103, 261…)
- You spent a lot of time considering conspiracy theories (anti-government) when looking at Team Blaze. Can you share why this was such an important topic for you? (see lines 86-92)
- In Line 83-84, you say, "that's not surprising; that is a good flag" - what does surprise mean for you in your analysis? Is it something you ignore, is it an outlier, is it something to follow-up on, possibly indicating a novelty, or something else?
- Line 98-100, you leap to solutions very rapidly here - what makes a solution recommendation (i.e., gate) good, in your opinion?
- In the workbook, there are a couple of sections called "What is missing." How did these help you in your analysis, if they did at all? If you discover something else "missing" from the model, what category does this go under (meaning, novelty)?

Specific Questions for Participant 2

- You describe your analysis as a "story that we are telling [and] how that story [is] propagating." Tell me more about why you describe analysis as a story.
- You recognize that the process is the process (moving from summary to meaning to novelty). Would you choose a different approach/framework for this project if the worksheet didn't constrain you with the built-in columns, etc.?

- In lines 59-60, you remembered you had some familiarity with Marburg and Ebola viruses. What would you do if the impact of these viruses wasn't familiar to you? How important is it to understand every reference or nuance in the data? What changes if you are wrong about acronyms or external research? (i.e., NPI on line 260)
- Lines 144-145, you reference a grid with compliance on the y-axis and trust on the x-axis. Did you ever draw that out, or did you just visualize it? What do you think this grid did for you as you moved further into the analysis? Were there conclusions already being drawn in your mind? Did you hypothesize that this grid would get you to conclusions faster?
- What makes a good scenario different from a bad scenario? (line 310)
- I notice many of your meaning-to-novelty thought flow follows a cause-effect relationship. Talk to me about that. (line 336, 341, 364)
- Line 439-440, you decide that "meaning" is the analyst's interpretation of the summary. Can you explain more?
- Talk to me about the clusters you refer to in line 460. Are these clusters of codes? Clusters of interpreted meanings? What are you clustering?
- So in line 496, you decide that something isn't really novel because we've seen it happen before. Talk to me about your expectation or definition of what truly novel means?
- I noticed it took you almost exactly 1 hour to be comfortable with knowing your "yardstick" (line 514), yet the whole analysis took 1 hour 6 minutes. And you went back and forth to summary and even novelty within that first hour. When did

you realize that the yardstick was complete and sufficient to measure the models accurately?

- In line 568-569, you recognized something missing by not being able to engage with other analysts - what are the pros and cons of working solo and working with a team?

Specific Questions for Participant 4

- I noticed two different ways that appeared to be a gap closer for you: The first is when you say something like "I'm not sure that is the case…" or some type of skepticism about the model (e.g., line 44, 49, 60-61, 250-251). The other is when you say, "that is interesting!" (line 11, 129, 139, 169…). What do you think you are doing at each of these points?
- You have a more fluid approach to summarizing, meaning, novelty. Can you talk to me about any method you might have that would put an idea firmly in one box versus the other? (Line 211, Team Scorch: "privatized tech emergence of protective immediacy."
- In terms of process, do you assess gates/flags in a separate pass-through, as an add-on to the main pass-through, or something else?
- Again in terms of process, talk to me about your findings tab → are they nested? What is more interesting, those farther right or the ones in the left column? (line 386)
- Do you ever ask: "what are we not asking?" What are we not talking about?"

- How would you describe the idea of novelty? Line 421, you used surprise as a criterion to separate an idea → is that part of novelty? In line 518, you use "something that is not obvious" as a criterion too.

Specific Questions for Participant 5

- You are a reductionist - you said before that you pull apart every piece of the system and put it back together - Can you talk me through why this method works for you? How do you use it to communicate with others the importance of what you found? More importantly, how do you reduce info load without reducing clarity?
- What were you looking for when you rewrote the summaries? What information did you leave out? Do you ever go back and follow up on any potential info you left out or emphasized?
- In what Round (summary, meaning, novelty) do you feel your yardstick is complete? How do you ensure everything is measured accurately?
- What do you think about during "pre-screening"? Are you already looking for clusters/themes, or are you just reading for familiarity?
- It appears that you weigh "by volume" or the number of sticky notes you have, and a smaller stack may indicate an outlier. How do you decide if an outlier is important rather than just something to ignore?
- Talk to me about your "constellation" idea (line 72). Describe how it allows you to see the connections or non-connected clusters.

- In lines 85-86, you talk about having a feeling something is a novelty, but there isn't enough data to call it a full novelty. What do you mean?
- You've done and seen threatcasting work before that have some of these same ideas: food insecurity underpinning a lot of other insecurities; trust in gov't; etc. – how much do you reflect on previous work, previous findings to make these findings in this project? The question becomes: how much does your previous work influence your current project?

APPENDIX D

INTERVIEWS WITH FUTURISTS – SUMMARIZED FINDINGS

The following lists are analytical summaries of how participants chose to describe the post-analysis process, their role in conducting foresight work, and attributes of a futurist. “P1” is shorthand for participant 1, “P2” for participant 2, and so on.

Describing Round One: Summarizing

P1: “help break down whatever problem ...from the micro-level down to the point of view level and look at problems that affect even just a person”

P1: “I just break down what the scenario is”

P2: Right data

P2: “true to what you can determine is the spirit of their argument”

P2: “condense without smoothing”

P2: capturing the core story

P2: the details of granularity develop the story of a person

P2: 90/10 analytics/imagination

P4: Ensuring “I get everything right”

P4: extraction, put a new lens on, switch context

P4: how do I put the human back into the story?

P4: understand what the findings need to look like and prepare written descriptions to make the map to there clear

P4: efficiency: “how can I use that to help guide what I need to pull out?”

P5: First round of “sifting”

P5: counting the number of instances of an idea lends a sense to its importance

P5: be prepared to be a data junky

Describing Round Two: Finding Meaning

P1: “Interesting” means a “seemingly small thing in this scenario with a bigger signpost”

P1: “as you’re going through the rest of it, either realize that there’s more of it, of this category or this flag”

P1: “things that popped up in the data that were social...that was right there in the data…”

P1: using things in current events and the news to influence thinking

P1: “what I got out of the scenario, and this can be similar to a previous scenario”

P2: Interpretation, own experiences, imagination, creativity come into play

P2: look for implications of the data within the model

P2: 80/20 imagination/analytics

P4: Finding patterns

P4: “what am I reading into this?”

P5: Uses visualizations (constellation) mapping to see where ideas are connected

Describing Round Three: Finding Novelty

P1: “where the data shouldn't be similar as it is supposed to be a novel finding or piece of information that is different than the others”

P1: Try to avoid finding data to confirm the novel idea: “I don't try to come up with an overall novel finding until I have all the information because otherwise, I can get stuck on trying to keep that novel idea and put the proceeding data into that idea instead of the other way around.”

P2: Finding what isn’t in the data

P2: the bigger things we aren't seeing

P2: something I haven't seen before in my corpus of knowledge

P2: realize the star you are looking at is not a star but a fully functioning death star!

P2: Emergent property of the process

P2: creating a door instead of a mirror

P2: drop away some assumptions and let thinking be more unconstrained

P2: equal parts analytics, imagination, responsibility

P4: Also finding patterns

P4: All the signs say something is possible, "but no one's talked about it yet"

P4: "what's new about this that I've never thought about before or that we haven't seen before?"

P4: pushing past the obvious - throw out your first ideas because they'll never be new

P4: "get out the kind of crap that you always think about and to things that haven't really stretched your brain today"

P4: not regurgitation of something that has already been written

P4: may make people uncomfortable

P4: "why will this thing add new value to the world? Because it's not just about synthesizing what people wrote, the output should add new value."

P5: May not be the big finding that is very declarative, but it's still attached and might only be "second sentence"

P5: outliers might not fit because my own knowledge is lacking

P5: "I still feel like it's going to matter," and perhaps only to one reader who knows how it might be relevant

Labels of Foresight Work

P1: Practitioner

P1: Futurist foresight practitioner

P2: Skeptimist: “Optimistic skeptic”

P2: “I see and am concerned about the worst in humanity...we are both our own worst enemies and our only hope”

P4: Business strategist

P4: design innovation

P4: foresight strategist

P5: Weirdo

P5: Ecosystem producer

P5: “My role is working with all the humans, the data, the content, and bringing all of those things together to move the process collaboratively forward”

Attributes of a Futurist

P1: Analytics

P1: Imagination

P1: Responsibility

P1: training to be as objective as possible

P1: subjective through at least experience

P2: Curiosity

P2: “neuro fluid” (able to hold simultaneous possibilities in mind)

P2: relentless/ruthless

P2: courageous

P4: Curiosity (a broad curiosity of all topics)

P4: humility

P4: rigorous

P4: a little bit creative

P5: wildly open

P5: permission to be big, wild, imaginative thinkers

P5: diversity of thought

APPENDIX E

IRB EXEMPTION

ASU Knowledge Enterprise Development

EXEMPTION GRANTED

Andrew Maynard
Global Futures, College of (CGF)
480/727-8831
Andrew.Maynard@asu.edu

Dear Andrew Maynard:

On 2/8/2021 the ASU IRB reviewed the following protocol:

Type of Review:	Initial Study
Title:	Threatcasting Analysis Best Practices
Investigator:	Andrew Maynard
IRB ID:	STUDY00012743
Funding:	None
Grant Title:	None
Grant ID:	None
Documents Reviewed:	• Threatcasting_consent_5-Feb-2021.pdf, Category: Consent Form; • Threatcasting_interview_themes_5-Feb-2021.pdf, Category: Measures (Survey questions/Interview questions /interview guides/focus group questions); • Threatcasting_IRB_Protocol_v2.docx, Category: IRB Protocol; • Threatcasting_recruitment_email_5-Feb-2021.pdf, Category: Recruitment Materials; • Threatcasting_scenarios.pdf, Category: Other; • Threatcasting_supporting_documents_5-Feb-2021.pdf, Category: Technical materials/diagrams;

The IRB determined that the protocol is considered exempt pursuant to Federal Regulations 45CFR46 (2) Tests, surveys, interviews, or observation on 2/8/2021.

In conducting this protocol you are required to follow the requirements listed in the INVESTIGATOR MANUAL (HRP-103).

If any changes are made to the study, the IRB must be notified at research.integrity@asu.edu to determine if additional reviews/approvals are required. Changes may include but not limited to revisions to data collection, survey and/or interview questions, and vulnerable populations, etc.

Sincerely,

IRB Administrator

cc: Jason Brown
Jason Brown
Joshua Massad

BIOGRAPHICAL SKETCH

Jason C. Brown hails from Etna, California. He is an actively serving Lt. Col. in the U.S. Army and is a decorated combat veteran with over 20 years of service and multiple deployments to Iraq and Afghanistan. While in the Army, Jason has served as a tank platoon leader, squadron intelligence officer, company commander, instructor, and information warfare officer, among other staff positions. Before his work at ASU, he served as the U.S. Cyber Command liaison to all U.S. forces in Afghanistan. He will return to the cyber force as a researcher and instructor at the Army Cyber Institute at West Point. He holds a bachelor's degree in Russian studies and master's degrees in information technology and information operations. Jason's hobbies include playing, coaching, and officiating volleyball, where he is a certified USA Volleyball and Arizona Interscholastic Association referee, playing the cello, and serving in his church. Jason has been married for 18 years and has three teenagers at home.