United States Military Academy
USMA Digital Commons

ACI Books & Book Chapters | Army Cyber Institute

3-2020

Threatcasting in a Military Setting

Natalie Vanatta
natalie.vanatta@westpoint.edu

Brian David Johnson
Arizona State University, bdj.futurist@gmail.com

Follow this and additional works at: https://digitalcommons.usmalibrary.org/aci_books

 Part of the Other Applied Mathematics Commons, and the Other Social and Behavioral Sciences Commons

Recommended Citation

Vanatta, Natalie and Johnson, Brian David, "Threatcasting in a Military Setting" (2020). *ACI Books & Book Chapters*. 19.
https://digitalcommons.usmalibrary.org/aci_books/19

This Book is brought to you for free and open access by the Army Cyber Institute at USMA Digital Commons. It has been accepted for inclusion in ACI Books & Book Chapters by an authorized administrator of USMA Digital Commons. For more information, please contact dcadmin@usmalibrary.org.

SERIES IN OPERATIONS RESEARCH

HANDBOOK OF MILITARY AND DEFENSE OPERATIONS RESEARCH

Edited by

Natalie M. Scala

James P. Howard, II

CRC Press
Taylor & Francis Group

A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2020 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

International Standard Book Number-13: 978-1-138-60733-0 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Chapter 6

Threatcasting in a Military Setting

Natalie Vanatta and Brian David Johnson

6.1 Introduction

The intersection of digital and physical security is critical to the future of our military and national defense. Impending technological advances widen the attack plain over the next decade including cyber-social, cyber-physical, and cyber-kinetic attacks. Visualizing what the future will hold, and what new threat vectors could emerge, is a task that in the 21st century, traditional military planning mechanisms struggle to accomplish given the wide range of potential issues.

In February 2011, Secretary of Defense Robert Gates told West Point cadets:

> *When it comes to predicting the nature and location of our next military engagements, since Vietnam, our record has been perfect. We have never once gotten it right, from the Mayaguez to Grenada, Panama, Somalia, the Balkans, Haiti, Kuwait, Iraq, and more — we had no idea a year before any of these missions that we would be so engaged*
>
> (Zenko, 2012).

Understanding and preparing for the future operating environment is the basis of an analytical process known as Threatcasting. Arizona State University's School for the Future of Innovation in Society, in collaboration with the Army Cyber Institute at West Point, use the Threatcasting analytical process to give researchers a structured way to envision and plan for risks ten years in the future. The Threatcasting analytical

process assists and enables practitioners to imagine enemy innovations before they happen and identify actions that can disrupt or respond to these enemy innovations. For many organizations, the scope of this problem can seem overwhelming.

Threatcasting uses inputs from social science, technical research, cultural history, economics, trends, expert interviews, and even a little science fiction. These inputs allow the creation of potential futures. By placing the threats into an effects-based model (e.g., a person in a place with a problem), it allows organizations to understand what needs to be done immediately, and also in the future, to disrupt possible threats. The Threatcasting analytical process also exposes what events could happen that indicate the progression toward an increasingly possible threat landscape.

The Threatcasting analytical process draws strength from futures studies, a field that provides theoretical and applied tools designed to shed light on deep uncertainties and complexities that futures hold. Foresight tools are rooted in exploratory, rather than predictive methods of futures thinking, learning, and strategy in order to prepare and plan for long-term outcomes that are difficult to imagine and impossible to predict (Bell, 2009). Such methods often stand in contrast to causal, linear, "plan and predict" thinking that characterizes many contemporary practices of making and knowing futures.

As national security and technological possibilities change rapidly, new threats and opportunities become ever-present. Threatcasting is a means to make sense of potential military futures so that relevant institutions can anticipate, manage, and navigate both the uncertainty and complexity ahead. This chapter will explain the Threatcasting analytical process as well as use the weaponization of artificial intelligence (AI) in a supply chain setting to demonstrate how Threatcasting has been applied and used in the real world. Specifically, we will outline two case studies where the process was applied with specific results. One case study focuses on the digital and physical supply chain in private industry (Cisco Systems) and the second investigates similar threats to the military's supply chain (Military Logistics Officers).

6.2 Emerging Need for Foresight

In the last few decades of the 20th century, foresight and long-term strategic planning were introduced into corporations and private industry. The practice was pioneered and used for decades in the specific industries that needed to make decisions that might not pay off for five to ten years (e.g., energy, city planning, etc.). With the invention and proliferation of the personal computer and the internet, a wider range of organizations saw disruption and innovation happening at an increasing rate. This was especially apparent in the high tech or Information Technology (IT) industries (Popper, 2008). These companies' long lead-times in product development roadmaps means that they need to know what people would want to do with technology five to ten years in advance. Additionally, because of the complexity of these products, many of these companies needed to explain how a new product or service might be used years before it was ready for market. Ecosystems with multiple players needed to be convened around a vision for the future for the product to be successful.

Taking a cue from the high-tech industry, as companies prepared for the technological gains and advances in the 21st century paired with the seismic shock and loss of the Great Recession, a wider range of corporations and organizations began to look to strategic foresight to plan for the future, and to make sure that they were the disruptor in their markets.

As these corporations hired foresight professionals, they learned that the results of the process gave them a vision for possible futures/products and informed their current business strategy. Human Resources (HR) professionals began to use these long-term visions to prepare their hiring and training strategies. Mergers and Acquisition departments used the output to target early stage companies and startups for either investment and/or acquisition. Legal and Intellectual Property groups began to use the output to increase the company's patent portfolio and to develop "future proof" contracts. These are long-term contracts and agreements between companies that might span five to ten years and have language in them that prepare for possible innovations and technologies that will be released multiple years into the future.

Similarly, in the 21st century, the landscape and possible problems that will need to be addressed by the operations research community are growing more complex. Operations research, as an academic discipline, is about applying advanced analytical and mathematical methods to make better decisions in relation to complex problems. Within operations research, foresight could be used as a tool to provide richer data sets, as well as greater detail and definition to these possible and probable threat futures.

The threat landscape in the 21st century is agile, adaptive, fast-moving, and enhanced by evolving technology. These factors create a larger pool of threat adversaries that could have a massive effect on the United States (US) via cyber means, which were previously only seen via kinetic means, effectively lowering the barrier to entry for non-nation state actors to influence the US. Secretary of Defense Chuck Hagel articulated these threat concerns in 2014, with the creation of a third offset strategy. Offset strategies encourage innovation with an appropriate combination of technologies, and operational and organizational constructs, to achieve decisive advantage against our adversaries in peacetime to remain in a position of world power. A key piece of the third offset strategy is to develop cutting edge technologies in the field of robotics, autonomous systems, miniaturization, big data analysis, and advanced manufacturing to incorporate into military operations. Additionally, to ensure the US recruits and retains the individuals that are capable of these breakthroughs, to be able to respond to our adversaries.

Similarly, these agile and adaptive threat concerns are also reflected in the soon-to-be-published multi-domain operations (MDO) v1.5 which General Stephen Townsend states is the "evolution of a larger effort to develop and revise Army thinking and requirements to defeat multiple layers of stand-off in both competition and conflict" (Judson, 2018). MDO now recognizes that while we might have originally envisioned the future to be fighting across all domains – land, air, sea, space, and cyber – we really need to be prepared for a highly contested environment where the joint forces won't have dominance across the entire spectrum. This is a different future environment that our current military forces have not faced in their lifetimes – full of unknowns and evolving threats that are hard to define.

Current operations research processes and procedures are necessary, but do not identify the futures threat landscape. Therefore, the processes of foresight and Threatcasting can enable the traditional practice of operations research and fill gaps that currently exist. For example, Threatcasting can provide a broader range of "alternatives," a wider range of threats and futures to be analyzed, and probable futures. Furthermore, with these possible threats identified, practitioners can use backcasting (a process that defines time-phased alternative-actions) to imagine how to disrupt, mitigate, and recover from the threats. This provides greater clarity for possible actions and uncontrollable externalities for Optimization and the final data analysis after data-farming.

6.3 Definition of Threatcasting

The Threatcasting analytical process is a four-phase methodology that aligns with the body of academic work within the foresight and futures community. The process allows practitioners to approach military futures not in a vacuum nor with only an understanding of a small portion of the problem but instead with a systems-view to enable the user to grapple with complexity, uncertainty, and risk. The Threatcasting process begins with a research synthesis phase, which draws from the Delphi method (Linstone & Turoff, 2011). This is followed by the forecasting phase, which utilizes elements of scenario building and science fiction prototyping (SFP). Phase three is the time-phased, alternative-action definition (TAD) phase which generates multiple backcasts. The final phase consists of data analysis, technical documentation, and communication of both the future threats and the actions to be taken. A graphical depiction of the process is seen in Figure 6.1.

Ultimately, Threatcasting is a human-centric process. Practitioners' participation in the modeling session is essential. Bringing together individuals from the military, government, academia, and private industry, with the objective to envision possible threats ten years in the future, gives each group the ability to brainstorm what actions can be taken to identify, track, disrupt, mitigate, and recover from the possible threats in a way that is more comprehensive than if each group had done the modeling on their own.

6.3.1 Phase Zero

A fundamental component of the Threatcasting analytical process is selecting the appropriate research inputs to feed the process. These focus themes are selected to explore how their evolution from today contributes to the future, and how the intersections of the focus areas' growth modify each other. To select these themes, senior leaders inside the problem space and thought leaders outside the problem space are consulted on what "keeps them up at night" or what they feel no-one is focused on yet, in order to determine the severity and urgency of the proposed themes. These curated themes are then explored by Subject Matter Experts (SMEs) in a 10–15-minute recorded presentation to be used in Phase One.

When an organization is modeling possible threats, there is a tendency to try and "boil the ocean." Many groups attempt to comprehend and model all possible threats.

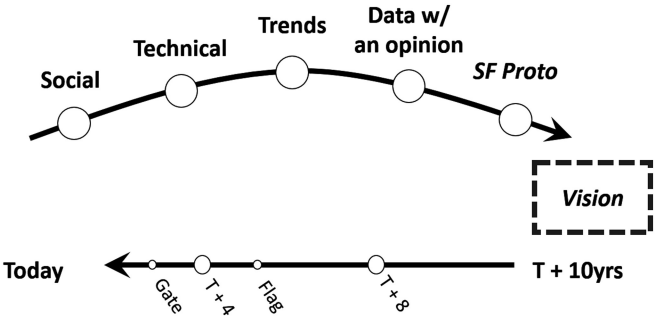

FIGURE 6.1: Threatcasting methodology (Johnson et al., 2017).

The Threatcasting analytical process ensures that groups are focused or "curated" only on specific threat areas. This enables the team to not only envision quality futures, but also get into designing potential disruption, mitigation, and recovery actions against these threats, as they are not attempting to solve all the problems in the world, just a curated set.

6.3.2 Phase One

Research synthesis is the first phase of the Threatcasting analytical process. The purpose of this phase is to allow each small group of practitioners to process the implications of the SME provided data while gathering the intelligence, expertise, and knowledge of the participants. The output of this phase becomes the raw data that is used to inform subsequent phases.

During this phase, all participants listen to each SME's presentation (curated from Phase Zero) and take notes. At the end of the presentations, they break into assigned small groups and using a specifically designed Research Synthesis Workbook (RSW) are led through an exercise to process and discuss the presentation material. Within the groups, they identify the key elements provided by the SMEs and discuss the larger implications of those elements in the future, based on their expertise. Additionally, the group characterizes each element as either positive or negative, and then lists ideas for what "we" should do about it. The "we" is purposely broad, as the input can be personal to the small group, the collected team in the room, the larger organization, or the entire human race. All of this information is captured in the RSWs.

The output of the research synthesis phase is a numbered list of these key points from the SMEs as determined by participants. Therefore, each circle in the top arc of Figure 6.1 is populated with a list of key considerations.

6.3.3 Phase Two

The core of the Threatcasting analytical process begins with phase two. The purpose of futurecasting is to model the future environment, based upon data compiled in the RSWs. These views of the future are effects-based models, meaning that the group is not modeling a specific threat or future first; they are exploring the layered effects that this threat will have on a single person, in a specific place. Threatcasting harnesses the futures wheel concept (Innatullah, 2008) for imagining and exploring, and further extends it beyond a single effect of a future event. This creates a more detailed effects-based model that ultimately explores the threat in greater depth.

Futurecasting is drawn as the upper arc in Figure 6.1, resulting in the "dashed" future at the far right of the figure. Each small group of participants generates this future in the form of a science fiction prototype (SFP). SFPs incorporate storytelling as a means of introducing detail into the future models and empowering the investigation into the human impacts, as well as scrutinizing the political, ethical, legal, and business impacts of these futures (Johnson, 2011, 2013). The SFP process follows a simple set of rules, as all stories have similar ingredients that drive the narrative, making them engaging enough for the reader to suspend disbelief with a structure to support potential plot resolution. Whether it is literature, motion pictures, or comic books, all stories or narratives contain a person, in a place, with a set of problems. Therefore, the output of phase two is a detailed outline for a specific future that the participants can then envision.

6.3.4 Phase Three

The third phase is the time-phased, alternative-action definition (TAD) process. TAD allows participants to explore multiple time-based futures and actions that can be taken to disrupt, mitigate, and recover from the future threats they have identified. Drawing from the practice of backcasting (Robinson, 1990, 2003), TAD provides multiple "backcasts," over a variety of timeframes and possible actions creating a multi-verse of options, plans, and strategies. Broadly speaking, Threatcasting engages the backcasting methodology by asking participants to work backwards in time from their one established future to identify what could be done to disrupt, mitigate, and/or recover from their defined threat. This is visualized as the backwards arrow in Figure 6.1. Participants are explicitly asked to imagine and place two types of indicators along their future trajectory: gates and flags.

Gates are actions (e.g., the use of technologies, capacities, systems) that defenders (government, military, industry, etc.) have control over that could disrupt, mitigate, and/or recover from the established threat. These are things that will occur along a concrete timeline from today (T) to T+10 years. Flags are events (e.g., economic, cultural, geo-political) or advances (e.g., technological, scientific) that defenders have no control over but once they occur, establish path dependencies with significant repercussions and consequence. Flags have an irreversible effect on the envisioned future and should be watched for as heralds of the future to come.

With the gates and flags established, the small groups then work from the future to the present to determine and timeline what specific actions (e.g., investments, organizational changes, technological development, security, policy) they might take to disrupt, mitigate, or recover from the threatcasted event. Thinking through concrete actions that would prevent their future threat gives participants the ability to understand how decision-making across time affects future outcomes. For the military, this provides a novel way to see how decisions to act today might help prevent tomorrow's threat.

One key benefit and output of the Threatcasting analytical process is its exploration of potential second- and third-order effects of these actions within the future. This is especially useful for large and complex military and business organizations. The SFPs craft a quick and easy way to understand the story, giving these organizations an efficient way to expeditiously understand threats and discuss what action(s) need to be taken.

6.3.5 Phase Four

Following the Threatcasting session, moderators use the RSWs as well as the small group future narratives (SFPs) as raw data for a synthesis session. Reviewing each workbook, the team of moderators look for patterns in the futures and for areas that were not explored.

The phases of the Threatcasting analytical process generate multiple futures and threats. In phase four, secondary research as well as the backcasting details from the practitioners give the moderating team the raw data needed to make specific recommendations for action in the near and long term. This post-analysis consists of multiple clustering and aggregation exercises to determine the patterns in all the recorded futures. These clusters are then examined in light of the SME presentations, looking for possible inconsistencies or areas that need more clarification. Additionally, the team highlights SME themes that the groups did not model but were strong components of

the expert presentations. Combining all of these together, the team compiles a technical report with specific recommendations for next steps and areas of action, informed by the participants.

Additional details about how a practitioner can execute the phases of the Threatcasting analytical process can be found in the *Journal of Defense Modeling and Simulation* (Vanatta & Johnson, 2019). This chapter will now present case studies on the application of the Threatcasting analytical process and its importance to the field of operations research.

6.4 Supply Chains Defined by Industry and the Military

Stated simply, a supply chain is a network or system of companies, organizations, people, activities, information, and resources used to move products and sometimes services from single or multiple suppliers to an organization or customer. Over the last few decades, the subject of supply chain and the idea of supply chain management have become popular topics in both military and private industry.

In the private sector, this has been driven by globalization and the ability for a single organization to source different aspects of a product from multiple suppliers across the globe.

> *Corporations have turned increasingly to global sources for their supplies. This globalization of supply has forced companies to look for more effective ways to coordinate the flow of materials into and out of the company. Key to such coordination is an orientation toward closer relationships with suppliers. Companies in particular and supply chains in general compete more today on the basis of time and quality. Getting a defect-free product to the customer faster and more reliably than the competition is no longer seen as a competitive advantage, but simply a requirement to be in the market. Customers are demanding products consistently delivered faster, exactly on time, and with no damage. Each of these necessitates closer coordination with suppliers and distributors. This global orientation and increased performance-based competition, combined with rapidly changing technology and economic conditions, all contribute to marketplace uncertainty. This uncertainty requires greater flexibility on the part of individual companies and supply chains, which in turn demands more flexibility in supply chain relationships.*
>
> (Mentzer et al., 2011)

Although similar in many ways, corporate supply chains differ from military supply chains in several ways. The size of the military supply chain is considerably smaller than that of private industry. Part of this constraint comes simply from need. The size of the market that a military supply chain is addressing is just smaller, as the military is less than 1% of the entire US population. This means that the addressable market could be seen as 99% smaller than private supply chains. However, there is an inverse effect at work in a military supply chain. Due to the nature of the "business" of the military, if the supply chain breaks down or is weaponized, the possible effects are not 1% of a similar disruption in the private sector. The effects would be far more dangerous and potentially destabilizing.

Another difference between military and private sector supply chains is the barrier of entry to become a part of that supply chain. To receive a government contract and become a part of supply chain system, there are a greater number of requirements and associated regulations. Therefore, the makeup of the military supply chain is constrained by the number of organizations that can meet these requirements. The private sector supply chain is for the most part market-driven. Some private industries are regulated more than others, but these regulations come from governments. The military supply chain is constrained by itself, with a broader set of goals beyond its market-driven counterparts. The Federal acquisition process imposes regulations and laws upon the military to accomplish things like "spread the wealth" that are goals far different than a market-based supply chain.

Finally, military supply chains are also constrained by their inability to pull any manufacturing or ownership inside the organization. For example, global advertising and search giant Google, made the strategic decision to own their undersea cables to protect their business interests. Similarly, the company decided to manufacture their own hard-drives to meet their operating specifications in their data centers (both for efficiency and security). In another high-tech example, Apple started making its own microprocessors when they realized the risk they were taking on by allowing others to craft them. Unlike these examples, the military does not have the ability to resource their own supply chain and become manufactures of key components of systems. They must rely on a private, global industry to meet their needs.

The weaponization of any organization's supply chain and logistics systems poses a significant threat to national and global economic security. The very systems that are the engine of economies and the lifeline of goods and services to the world's population could, and most probably will, be turned against the very people and organizations that they serve. This new threat landscape and associated challenges will affect industry, militaries, and governments through loss of revenue and productivity and even loss of life. This weaponization will allow adversaries, whether they are criminal, state-sponsored, terrorists, or hacktivists to transform these systems from engines of productivity to enemies on the inside.

6.5 Threatcasting Applied in Industry

The Threatcasting analytical process has been used in industry for over a decade. Its use started in Silicon Valley with companies like microprocessor manufacturer Intel Corporation and software design tools company Autodesk. These organizations used the Threatcasting analytical process to build better products and solutions for customers. Much of this work is kept confidential because it contains company secrets, product strategies, patents, and other intellectual property. Therefore, there is little specific documentation or case studies of Threatcasting use within private industry. There are examples of Threatcasting use in academia, including by legal scholars (Bennett & Johnson, 2016) and the body of work is increasing each year. Additionally, multiple academic and military institutions (e.g., Georgetown University, Arizona State University, the United States Naval Academy, the United States Air Force Academy, the United States Military Academy) have begun teaching the Threatcasting analytical process as a tool for students to explore complex and uncertain futures. Recently, two industry organizations have publicly discussed their use of Threatcasting and their results.

Cisco Systems is an American technology company that develops, manufactures, and sells networking and telecommunications hardware equipment. Inside the Silicon Valley-based company is their innovation lab called CHILL. CHILL stands for Cisco Hyper Innovation Living Labs. It is

> *an innovation capability that aims to disrupt through the development of businesses and joint projects in 48 hours. It's a unique and new project in its third year for Cisco and the brain-child of Kate O'Keeffe, Senior Director. Each CHILL Lab tackles a different topic facing the globe.*
>
> (Bonime, 2018)

The CHILL event was titled "Securing the Digitized Supply Chain Powered by Blockchain." The team

> *aimed to drive disruptive innovation with and for customers … which drive joint investment opportunities from multiple parties into projects or startups that get support. The partners for the Blockchain Lab included CitiBank, Intel, GE, and DB Schenker, among others.*
>
> (Wal-Aamal, 2017)

In preparation for the lab, O'Keeffe and team used the ASU's Threatcasting Lab report A Widening Attack Plain (Johnson, 2017a) to draw out specific threats and futures for the future of the digital supply chain. The authors of the report included experts from the government, military, private industry, trade associations, and academia. Specifically, the report explored the intersection between a global, digital, and automated supply chain, with the threats of cyber-attacks and terrorism.

Based upon the report, the CHILL team Threatcasted a future featuring a

> *state-sponsored terrorist attack using smart refrigerators and pantries that place excessive dairy and produce orders to a complex automated supply chain. With the roads and ports now clogged, the terrorists exploit a weakness in the Red Hook, New Jersey port system to sneak a dirty bomb into the country and detonate it in downtown New York.*
>
> (Johnson & Vanatta, 2017)

To better express this future in a short period of time, CHILL used the threat future as the basis for a science fiction prototype, "Two Days After Tuesday" (Johnson, 2017c). The goal was to develop and create a powerful narrative that would serve as a fact-based illustration of the future threats.

When asked about the effectiveness of the Threatcasting analytical process and the science fiction prototype, O'Keeffe said in an interview,

> *People aren't wired to imagine the future, ten or even five years out, which is a blocker to innovation … We need to create that world for them, so they can immerse themselves in this future scenario, making it immediately apparent what kind of solutions we need to prepare for that future.*
>
> (Johnson & Vanatta, 2017)

The result of the CHILL event was success. Five new business or product concepts were generated by the lab based upon the Threatcasting futures and received funding at the event. When asked about the effectiveness of the labs in an interview O'Keeffe replied,

> *In our last three Labs we invested in six outcomes, of which 2 are still existing today. CHILL is an important part of our innovation engine as Cisco spends $6 billion in R&D, $2.2 billion in venture capital, and $250 million investment fund and has invested in 100 startups.*
>
> (Wal-Aamal, 2017)

Cisco used Threatcasting and its derivative deliverables as an input to their innovation process while other organizations have used it to identify future threats to markets and entire industries.

The American Production and Inventory Control Society (APICS) is a trade association that provides supply chain, logistics, and operations management research, publications, education, and certification programs. The organization provides Threatcasting as a key offering to their members who are concerned with digital and cyber-attacks. For example, they conducted a Threatcasting workshop during their annual conference in 2019.

In each seminar a presenter or speaker leads the group of supply chain professionals through the Threatcasting analytical process and works to apply the results specifically to the attendees' possible and probable future threats.

APICS specifically focused on the TAD component of the Threatcasting analytical process to identify areas of strategic focus for their organization and the entire supply chain industry. The results of the TAD mapped multiple areas that touched on "urbanization, Africa, the young and elderly, women in global society, technological autonomy and intelligence, data, transparency, fully conscious consumerism, and the speed of change" (Proctor, 2017)

These two different applications of Threatcasting in industry illustrate how the process can be used to identify future threats to an organization or systems. Once these threats have been identified, the organization can explore how to track, disrupt, mitigate, and recover from those threats.

Additionally, the process can be used to generate raw material for existing organization processes and procedures, giving practitioners a new or different viewpoint to better capture the current and future shifting landscape.

6.6 Threatcasting Applied to the Military

The Army Cyber Institute (ACI) is a national resource for research and engagement to enable effective Army cyber operations in the future. Put another way, this small thinktank exists to prevent strategic surprise in cyberspace and ensure the Army's dominance by scanning new developments on a three-to-ten-year horizon.

Similar to the previous section covering industry's concerns, ACI wanted to empower change within its larger organization (US Army) to prevent, disrupt, mitigate, and/or

recover from these future threats and the impacts of the potential weaponization of Artificial Intelligence (AI). Like many challenges within the military domain, there is never a single solution. Many elements and factors are necessary to determine success. For instance, DOTMLPF (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities) is an acronym that Army leaders learn and adopt from their professional military education. The underlying idea is that multiple different facets and components go into developing a successful force. More importantly, that all aspects of DOTMLPF influence the end state and they also interact with each other (both negatively and positively). Threatcasting's Phase One builds on this military notion by harnessing the diverse SME domains to highlight how technology might evolve in the future, and how the other facts/domains might influence both the development and employment of the technology.

Exploring the future of military supply chains revealed several possible and probable scenarios. These included a future in which suppliers to the supply chain (such as a transportation company) embrace and implement advanced AI-driven automation. This high level of automation could include both the physical and the digital world. In the physical world, robots, self-driving cars, trains, and drones become the physical backbone for the movement of goods and supplies. In the digital world, AI is used to not only manage the physical autonomy but to make decisions and value calls that would have normally been taken on by humans.

This continued increase in automation will be driven by multiple factors. The first is a relentless drive for efficiency and cost-cutting measures. As budgets are tighter and the military is asked to do more with less, there is little choice but to automate as much of the process as possible. By removing the person from the loop, decisions can be made faster and the supply chain becomes increasingly optimized for speed and efficiency. These changes in society, culture, and economies influence the direction of the technology and its acceptance.

This relentless drive for efficiency exposes the supply chain to massive vulnerabilities. It is well known that a complex system, like a supply chain, cannot be designed for both efficiency and security (Johnson, 2017b). One needs to be sacrificed for the other. In this future scenario, security is sacrificed for efficiency. This becomes a direct threat to national security given the activities that are supported by commercial supply chains.

Therefore, the threats that the Threatcasting analytical process session produces, while not always focused on the military, can still be applied directly to military operations. A key component of Threatcasting is using a diverse group of participants to think about the future. Their diverse inputs can produce a wide variety of outputs and can be applied in a military setting. These future threats can be used even when their first instance was not in a military setting. SFP can take general Threatcasting results and make them more useful for a military audience. For example, the ACI used both the A Widening Attack Plain and The New Dogs of War: The Future of Weaponized Artificial Intelligence Threatcasting technical reports as the foundation of a targeted SFP workshop to create a tactically feasible, operationally correct vision of the future. The future operating environments outlined in these documents were then applied to military operations.

Over a two-day workshop, diverse military members (officers of all ranks, Marines and Soldiers, from each branch and many functional areas), with different experiences (both in terms of operational deployments, continents served on, and unit types)

gathered to "turn the crank" on the Threatcasting results. Namely, to apply the threats from previous Threatcasting sessions to the context of military understanding and operational environments. A series of graphic novellas and animated movies were produced, with the intent of educating Army leaders at all levels about the contested domain of cyberspace. They demonstrate how the adversary can affect our ability to fight and win our nation's wars, at home and abroad. These graphic novellas were also designed to spark innovative thinking amongst the force and across society to help prevent, detect, mitigate, and recover from these possible futures.

"Our thought was to put these stories out, spread these ideas into the ecosystem, and build a community," said Colonel Hall, director of the ACI. "Our hope is to influence our partners in industry and academia, as well as the junior leaders within the Army we believe will have to deal with these issues in the future."

11.25.27 is the story of Lieutenant Jenkins and her skeleton crew working on Thanksgiving Day to supervise the loading of military equipment that arrived two days late to the port. Without a second thought one of them tweets "Finally … Looks like I will get some turkey! #hatemylife" … and the attack begins. Months before, the Army's highly automated supply chain and the deployment planning system had been breached, turning them into a weapon for a local terror cell. Small errors and minimal oversight sent a deadly payload to the docks of Seattle, WA. A pair of autonomous drones fly on a collision course with a specially loaded railcar … millions will die. No one will ever forget 11/25/27. (Johnson, 2018)

"Graphic novellas are a medium with a rich tradition of use by the US Army," said Lieutenant General (Retired) Rhett A. Hernandez, former commander of the US Army Cyber Command.

> *For generations, the Army has successfully used this medium for conveying important messages across its force. Today, the Army Cyber Institute is continuing this tradition based on science fiction prototypes of cyber threats it may encounter on the future battlefields.*

6.7 Implications for Design

The Threatcasting analytical process and operations research intersect in some key areas: analysis of alternatives, wargaming, modeling and simulation, data analysis after data-farming and wrangling. For example, the process and output of Threatcasting can provide needed inputs to broaden the range of possible futures that are analyzed and eventually used for wargaming, while TAD can help clarify modeling and simulation impact decisions, as well as data analysis, after data-farming. Currently, the qualitative results of the Threatcasting analytical process cannot be mathematically validated; however, they are used as scenarios and inputs to quantitative models (e.g., agent-based threat modeling, risk analysis, gap analysis). With the increased use of Threatcasting within the discipline, future work is anticipated in this direction.

The primary goal of Threatcasting is to draw together a broad range of inputs to better define a wider range of possible threats in a specific area. For operations research, these inputs would provide the decision-maker more information and help screen out options when conducting an analysis of alternatives. These threat futures can also

provide a wider range of potential futures that can then be used for the multiple criteria decision analysis process. Additionally, the effects-based models that are at the center of the Threatcasting analytical process can provide a new lens for the practitioner who is using value focused thinking, allowing them to build design options based upon an individuals' or organizations' values and desired outcome.

Threatcasting's broader range of threats provide practitioners more diversity of possible situations and landscapes to feed into the design of wargames. Often when designing a wargame, operations research practitioners focus more on the execution of the wargame and what the adversary might do. But in order to have truly effective results, it is also important to base the foundation of the wargame on a broader, more diverse set of potential scenarios. Threatcasting can provide a high degree of detail to these future scenarios, giving greater real-world complexity, as well as more specificity to the output.

Once the threat futures have been defined and the backcasting has taken place, this new dataset can provide practitioners valuable inputs to key areas of operations research. The data generated for how to disrupt, mitigate, and recover from these threats provide a more robust input for modeling and simulation. The powerful narrative component of Threatcasting can feed into this step and provide more detail in the multi-domain battle space. The TAD time-based step function of backcasting provide practitioners more detail for modeling and simulation, and gives practitioners multiple approaches and timeframes for the modeling and simulation.

In the post-analysis of data, the transparent nature of the Threatcasting analytical process allows practitioners to monitor the accuracy of their models. Practitioners can examine the driving factors for a threat, looking for key flags or indicators that the threat is on its way to becoming a reality. Original sources can be checked, thus allowing for assumptions to be challenged and better analysis to be derived.

Ultimately, operations research seeks to deal with uncertainty. Using Threatcasting to illuminate a broader range of possible threats and actions to be taken to meet those threats means that the areas of uncertainty will shrink. Additionally, the Threatcasting analytical process allows practitioners to process a wide range of disparate inputs to understand a wider range of possible futures. In this way Threatcasting can be seen as a way to actually deal with and process uncertainty.

6.8 Conclusion

In this chapter we reviewed the Threatcasting analytical process in detail so that it can be applied to multiple areas of interest for operations research. The Threatcasting analytical process assists and enables practitioners to imagine enemy innovations before they happen and identify actions that can disrupt or respond to these enemy innovations. It is a needed process that produces results that can provide a basis for operations research in areas such as a concept of operations (CONOPs) development or resource allocation decisions.

Using the analytical process, practitioners can explore and comprehend the close ties between the advancement of technology and the potential effect that it could have on society, economies, and national security. To illustrate this, we applied the Threatcasting analytical process to specific problems in military and corporate supply chains, by focusing on the weaponization of AI. As an output of this work, we showed

the need for and motivation to create powerful narratives and fact-based illustrations that can provide leadership and decision-makers a concise and expeditious way to comprehend the results of the Threatcasting analytical process, and begin the initial steps of specific actions.

References

Bell, W. (2009). *Foundations of Futures Studies: History, Purposes, Knowledge. Volume I: Human Science for a New Era*. New York, NY: Taylor & Francis.

Bennett, M., & Johnson, B.D. (2016). Dark Future Precedents: Science Fiction, Futurism, and Law. In P. Novais and S. Konomi (Eds), *Intelligent Environments 2016*, (pp. 506–513). Washington, DC: IOS Press.

Bonime, W. (2018). Cisco CHILL to Tackle the Future of Work in 48 Hours. *Forbes*. Retrieved from https://www.forbes.com/sites/westernbonime/2018/02/04/how-cisco-chill-turns-ideas-into-companies-in-48-hours/

Inayatullah, S. (2008). Six Pillars: Futures Thinking for Transforming. *Foresight*, *10*(1), 4–21.

Johnson, B. D. (2011). *Science Fiction Prototyping: Designing the Future with Science Fiction*. San Rafael, CA: Morgan & Claypool.

Johnson, B. D. (2013). Engineering Uncertainty: The Role of Uncertainty in the Design of Complex Technological and Business Systems. *Futures*, *50*, 56–65.

Johnson, B. D. (2017a). A Widening Attack Plain. (Threatcasting Report: Army Cyber Institute). Retrieved from https://threatcasting.com/publications/

Johnson, B. D. (2017b). Efficiency is Easy to Hack. *Mechanical Engineering*, *139*(08), 38–43. doi:10.1115/1.2017-Aug-2

Johnson, B. D. (2017c). Two Days After Tuesday. Retrieved from https://www.threatcasting.com/about/sci-fi-prototypes/

Johnson, B. D., & Vanatta, N. (2017). What the Heck is Threatcasting? *Future Tense*. Retrieved from https://slate.com/technology/2017/09/threatcasting-in-futurism-attempts-to-imagine-the-risks-we-might-face.html

Johnson, B. D., Vanatta, N., Draudt, A. & West, J. (2017). The New Dogs of War: The Future of Weaponized Artificial Intelligence. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/1040008.pdf

Johnson, B. D. (2018). 11.25.2027. Retrieved from https://www.threatcasting.com/about/sci-fi-prototypes/

Judson, J. (2018). From Multi-Domain Battle to Multi-Domain Operations: Army Evolves its Guiding Concept. *AUSA*. Retrieved from https://www.defensenews.com/digital-show-dailies/ausa/2018/10/09/from-multi-domain-battle-to-multi-domain-operations-army-evolves-its-guiding-concept/

Linstone, H., & Turoff, M. (2011). Delphi: A Brief Look Backward and Forward. *Technological Forecasting & Social Change*, *78*(9), 1712–1719.

Mentzer, J. T. et al. (2011). Defining Supply Chain Management. *Journal of Business Logistics*. doi:10.1002/j.2158-1592.2001.tb00001.x

Popper, R. (2008). Foresight Methodology. In L. Georghiou et al. (Eds), *The Handbook of Technology Foresight* (pp. 44–88). Cheltenham, UK: Edward Elgar.

Proctor, J. (2017). Futurecasting the Supply Chain. *APICS SCM Now Magazine*. Retrieved from http://www.apics.org/apics-for-individuals/apics-magazine-home/magazine-detail-page/2017/01/30/futurecasting-the-supply-chain

Robinson, J. (1990). Futures Under Glass: A Recipe for People Who Hate to Predict. *Futures*, *22*(8), 820–842.

Robinson, J. (2003). Future Subjunctive: Backcasting as Social Learning. *Futures*, *35*(8), 839–856.

Vanatta, N., & Johnson, B. D. (2019). Threatcasting: A Framework and Process to Model Future Operating Environments. *The Journal of Defense Modeling and Simulation*, *16*(1), 79–88. doi:10.1177/1548512918806385.

Wal-Aamal, A. (2017). Cisco CHILLs about Securing Digitized Supply Chains on the Blockchain. [BLOG Post]. Retrieved from https://www.unlock-bc.com/news/2017-09-18/ciscos-chills-about-secure-digitized-supply-chains-on-the-blockchain

Zenko, M. (2012). 100% Right 0% of the Time. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2012/10/16/100-right-0-of-the-time/