2018

Threatcasting: a framework and process to model future operating enviornments

Natalie Vanatta
Army Cyber Institute, contact.cyber@usma.edu

Brain David Johnson
Arizona State University, brian.david.johnson@asu.edu

Technical Note

JDMS

Journal of Defense Modeling and Simulation: Applications, Methodology, Technology
1–10

DOI: 10.1177/1548512918806385
journals.sagepub.com/home/dms
SAGE

Threatcasting: a framework and process to model future operating environments

Natalie Vanatta and Brian David Johnson

Abstract

Threatcasting, a new foresight methodology, draws from futures studies and military strategic thinking to provide a novel method to model the future. The methodology fills gaps in existing military futures thinking and provides a process to specify actionable steps as well as progress indicators. Threatcasting also provides an ability to anticipate future threats and develop strategies to reduce the impact of any event. This technical note provides a detailed explanation of the Threatcasting methodology. It provides the reader with its connections to the current body of work within the foresight community and then explains the four phase methodology through the use of a real-life example.

Keywords

Threatcasting, cyber model, narrative, technology

1. Introduction

In 1941, Admiral King, Commander-in-Chief of the Atlantic Fleet, used a mathematical model to determine the United States' best ship building priorities to enable us to fight a two-ocean war. Using the resulting memorandum to the General Board, I have often discussed this model's potential construction in my introduction to mathematical modeling class at West Point. Unfortunately, attempting to model cyber situations, i.e., forecasting future needs and risks to direct efforts appropriately, is not as straightforward and intuitive.

Threatcasting, a new foresight methodology, draws from futures studies and military strategic thinking to provide a novel method to model the future. The methodology fills gaps in existing military futures thinking and provides a process to specify actionable steps as well as progress indicators. Threatcasting incorporates a variety of foresight methodologies, such as backcasting, scenario planning, and the Delphi method, into novel combination with traditional military strategic thinking and effects based modeling. The methodology provides an ability to anticipate future threats and develop strategies to reduce the impact of any event.

Researchers from Arizona State University's School for the Future of Innovation in Society and the Army Cyber Institute at West Point have used the threatcasting process over the last year to focus on the cyber domain and how it can revolutionize or paralyze the future operating environment.

2. Outline

This technical note provides a detailed explanation of the threatcasting methodology. It provides the reader with its connections to the current body of work within the foresight community and then explains the four phase methodology through the use of a real-life example. It concludes with future work planned over the next year.

Army Cyber Institute, Spellman Hall, West Point, NY, USA

Corresponding author:
Natalie Vanatta, Army Cyber Institute, Spellman Hall, West Point, NY 10996, USA.
Email: natalie.vanatta@usma.edu

3. Related work – strategic foresight

Strategic foresight and futures studies, while a relatively new academic field of study in comparison to mathematics, examine operational and tactical views of alternative futures and possibilities. While not a crystal ball, foresight allows professionals to mine the external environment for trends and issues, and leverage those insights to create a vision or multiple alternative visions of the emerging landscapes which enables the testing of current strategy, promotes the development of innovations, and motivates transformative change. Grappling with and anticipating a range of military unknowns through ''systematic and explicit thinking about alternative futures''[1] is the heart of threatcasting, and will be explored in depth later in this paper.

The relationship between futures thinking and military strategy is long-standing. Futures studies in the United States largely grew from military need following World War II (WWII).[1–3] Threatcasting has emerged in the last decade to fill the gaps in traditional foresight and military strategic frameworks exposed by the complexities of a shifting twenty-first century landscape.

Many elements within the traditional, academically accepted futures community are incorporated into the threatcasting methodology. Threatcasting utilizes prospective thinking. Prospective thinking involves thinking forward in time, challenging dominant expectations of what might occur, and proposing and exploring a wide-range of possible, probable, plausible, and preferable futures.[1,4–6] The art of backcasting is also incorporated in threatcasting. Backcasting is routinely used in long-term, complex problems that involve both technology and societal change as Robinson explains that ''the major distinguishing characteristic of backcasting analyses 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 desired future endpoint to the present in order to determine the physical feasibility of that future and what policy measures would be required to reach that point.''[7]

In addition, threatcasting evolves the notion of futures wheel which ''… seeks to develop the consequences of today's issue on the longer-term future. We can ask how a particular new technology might influence us 20 years from now. The futures wheel does not stop at first order impacts, but rolls along to second order impacts, and beyond. It intends to explore and deduce unintended consequences.''[8]

Elements of scenario planning are also incorporated into threatcasting to help ''break down existing mental models and rebuild another view of reality.''[9] To gather input from a broad range of global experts, threatcasting draws from the Delphi method,[10,11] not only to capture the research and world view of experts but also to gather contradictory opinions and perspectives on the future. Threatcasting is more than just a direct combination of the traditional futures techniques and methods. It combines these methods to take best advantage of their strengths while at the same time minimizing the effect of their weaknesses.

Ultimately, threatcasting combines traditional strategy with foresight to more accurately envision military futures and enable clear and measurable actions. Twenty-first century warfare is a complex human endeavor with multiple variables and uncertainties. Threatcasting and other foresight methodologies can help manage these variables.

4. Threatcasting methodology

Threatcasting's four-phase methodology aligns with the body of academic work within the foresight and futures community. The methodology approaches military futures not in a vacuum nor with understanding only a small portion of the problem, but rather takes a systems approach to grapple with complexity, uncertainty, and risk. The threatcasting processes begins with a research synthesis phase which draws from the Delphi method. This is followed by the forecasting phase which utilizes elements of scenario building and science fiction prototyping. Phase three is the time-phased, alternative-action definition (TAD) phase which generates multiple backcasts. The final phase of threatcasting consists of data analysis, technical documentation, and communication of both the future threats and the actions to be taken.

Threatcasting (Figure 1) operates using inputs from social science, technical research, cultural history, economics, trends, expert interviews, and science fiction. These various domain inputs allow the creation of potential visions of the future (focused on a person in a place doing a thing). Some of these resulting futures are desirable while others should be avoided. By placing themselves into the scenario, participants can imagine what can be done today and or multiple years from today to empower or disrupt that future. They can also determine what *flags*,

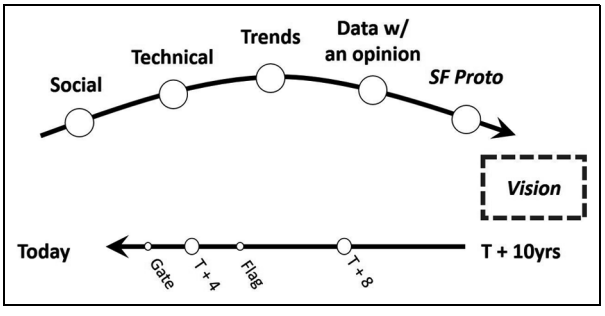

Figure 1. Threatcasting methodology.[12]

indicators or warning events, could occur that indicate that the environment is progressing or digressing toward or away from the modeled threats.

The threatcasting methodology is distinct from traditional military notions of military thinking, planning, and modeling. Not only does the methodology combine both linear and creative thinking it also requires that a diverse set of practitioners, from both inside and outside of the military gather and collaborate. This diversity of participants and the multidisciplinary nature of the sources it draws upon paired with multiple guided exercises to explore possible threats enable groups to envision a complex and evolving threat landscape.

4.1. Threatcasting participants

Threatcasting sessions typically take place over a specific time, normally one to two days. The participants come together in a single place, a physical or virtual space, to listen to curated research around a specific threat topic, collaborate in small groups and report out. The requirement for diverse participants (in age, experience, and education) in a threatcasting session reflects the methodology's human-centric process. As threatcasting is a theoretical exercise undertaken by practitioners, it is vital that the majority have domain knowledge of how to specifically disrupt, mitigate, and recover from the theoretical threat futures. However, a few participants curated can be outliers, trained foresight professionals, and young participants for a fresh and multi-generational perspective. Regardless of the problem set, workshop participants are assigned into three- to four-person groups for the entirety of the process. Small groups assure that every member can express themselves and promote in-depth discussion and debate.

4.2. Timelines in threatcasting

Threatcasting focuses on ten years in the future. This is a conscious decision in order to reduce innate biases from participants and to overcome plausibility concerns. Envisioning ten years into the future is an intellectually freeing experience, allowing participants to imagine a broader range of futures beyond their current state. The ten year timeline is typically past the duration of:

- political administrations,
- a corporate executives appointment,
- the longevity of participants' current superiors, and
- the life of any project that most participants are currently working.

Therefore, participants can free themselves from this baggage (their emotional connections to the present) and think about the future. Conversely, ten years is not so far in the future that the only things that make sense come straight from the pages of a science fiction novel. Ten years is also the sweet spot beyond where the operational military force is looking but before where the long-term thinking of U.S. Army Training and Doctrine Command (TRADOC) picks up.

4.3. Threatcasting themes

A fundamental component of the threatcasting process, like all foresight work, is selecting the appropriate research inputs to feed the future modeling. If the threat landscape is too broad, it is hard for participants to focus and typically the results are not as detailed. To overcome this challenge, threatcasting sessions revolve around a small number of primary themes. These themes are selected to explore how their evolution from today contributes to the future but also how the intersection 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 has focused on yet. This process allows workshop leadership to determine the severity and urgency of the proposed themes.

The themes are typically presented as 10–15 min prerecorded videos by subject matter experts (SMEs). In these, SMEs discuss the future challenges and/or direction they see their field moving over the next ten years and the considerations that participants should take into account during their modeling.

5. Threatcasting explained

The following sections of the paper provide a description of the four phases of threatcasting illustrated by an example from a threatcasting session, Threatcasting West 2017, conducted by the authors on a military problem.[12]

Threatcasting West 2017 focused on exploring complex defense issues such as the advancement of artificial intelligence (AI), the diminishing ability to conduct covert intelligence gathering, the growing complexity of code, and future division of work roles between humans and machines. Conducted in Tempe, Arizona, the workshop had 47 participants with diverse backgrounds (e.g., government, military, corporations, trade associations, nonprofits, and academia).

5.1. Phase one: research synthesis

Research synthesis is the first phase of the threatcasting methodology. The purpose of this phase is to allow each small group 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 material that feeds subsequent phases. During this phase, all participants listen to each SME's presentation and take notes. At the conclusion of the presentations, they break into assigned small groups and using a predesigned research synthesis workbook (RSW), are led through an exercise to process and discuss the research they have just seen. Within the groups, they identify key elements and discuss the larger implications of that element in the future, characterize this as either positive or negative, and list 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 information is captured by the small group scribes in the RSW during their exploration. The RSW allows for the documentation of the important data points from the research presentations as well as the opinions and views of the participants assembled in the room. Incorporating participants' insights and synthesis of SME opinions elevates this phase beyond typical Delphi techniques. Once these ideas are documented, the larger group re-convenes to share their analysis assignments. The output of the research analysis 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 1 is populated with a list of key considerations.

5.1.1. Example: phase one. For Threatcasting West 2017, six SMEs provided insights on the following topics (see Appendix 2 of the technical report by Johnson et al.):[12]

1. How to think about interrogating AI.
2. How to build AI without losing control over it.
3. Fourteen cyber considerations for humans.
4. How to approach threatcasting from an economic perspective.
5. The growth, impact, and future of applying AI to real world industries.
6. Key ideas from various expert interviews regarding cyber growth and our relationship with machines.

Table 1. Count of synthesized SME data points from Threatcasting West 2017.

SME	Number of synthesized points
SME 1	19
SME 2	15
SME 3	10
SME 4	15
SME 5	11
SME 6	20

Given these initial SME insights, Table 1 displays the number of synthesized points the participants felt would have a bearing on the development of future operating environments. The specific points can be found in Appendix 3 of the technical report.[12]

5.2. Phase two: futurecasting

The core of the threatcasting methodology 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 for imagining and exploring,[8] but 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 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 scrutinize the political, ethical, legal, and business impacts of these futures.[13,14] The science fiction prototyping 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.

The diversity of SME-inspired data points, drawn from the RSWs in phase one, are used to build the future scenarios' conceptual boundaries and framework. Each small group randomly selects data points from the SME presentations by rolling a multi-sided die whose numbers correspond to the specific data in the workbooks. Using dice ensures randomness and expands the possibility space while disabling participants from selecting data points that fulfill their particular images of the future.

The intersection of the SME data points and the commentary around implications give the participants the raw materials to create a future that is plausible and based upon current research. After establishing a mental visualization of the environment, the group imagines a specific person living in that future. The group envisions who the character is, their family, and the broader community with which they identify. Then the group explores where the character

lives, what the character thinks about their occupation, and visualizes what constitutes their normal way of life. This provides the foundation of the SFP – a person, in a place, doing a thing.

The physical or digital instantiation of the problem caused by the threat is the 'event'. To better model and understand the event, the small group is asked a series of questions that are designed to push the participants to add as much detail as possible to explore and explain their futures. Going beyond the military decision making process (MDMP)'s ''5Ws'' of traditional information gathering (who, what, when, where, why), threatcasting prompts are specifically designed to create a more well-rounded narrative describing the complexity and uncertainty of the threat and operating environment.

Then, as in all good science fiction stories, the perspective changes and the 'event' is seen from the adversary's perspective. Groups are asked to explore potential roadblocks or barriers and think about new business models and practices that would enable the event. They imagine what sociotechnical systems and discrete technologies would help facilitate the threat and what support systems are required for it to thrive. Finally, they think about the training necessary to enable this threat. From a military perspective, the groups look across the entire DOTMLPF (doctrine, organization, training, materiel, leadership, personnel, facilities) spectrum.[15] This change in perspective helps the small group to better define the threat, visualize the adversary's motivations, and understand their desired end state.

While the small groups are creating narratives of the future, moderators circulate to answer any questions. The moderators', typically trained futurists, primary role is to monitor the progress of each group and interrogate them on the validity, plausibility, and accuracy of their models. The moderator asks leading questions to challenge the group's mental models, assumptions, bias, and expand the breadth and depth of plausible futures envisioned. The end state of the futurecasting phase is that each small group has created a story about the future. Using storytelling and SFP with a specific arc provides the scaffolding needed to clearly articulate the world the character lives in and enables participants to center their future understanding on humans. As a result, clear and explicit connections are easily drawn between the current world and the world as envisioned through the threatcasting exercise.

5.2.1. Example: phase two. Continuing with our illustration from Threatcasting West 2017, small group #1214's results will be used to illustrate futurecasting. The group rolled the 20-sided die and incorporated the following six SME concepts into their future environment: (1) AI is another manifestation of what it means to be human; (2) there is an ongoing unregulated arms race to create the first super-AI; (3) cleared individuals in the Department of Defense are more at risk from adversaries and bad actors than ever and it's getting worse; (4) organizations must re-examine economic and risk models; (5) the next generation of AI will be adaptive, self-learning, and intuitive and there will be a corresponding metaphysical ''singularity'' among them all; (6) and there will be a society of modern separatists that have rejected AI and a digital existence.

Given the diversity of the small group construction in Threatcasting West 2017, no restrictions were placed on whom the specific person must be or where they live. Therefore, a handful of the groups, including #1214, chose to model a person living outside the United States. Threatcasting does not require fictional actors to be U.S. citizens or part of the Army because threats come from a variety of different places, in a variety of different ways, and at a variety of different times. In threatcasting, the narratives and details of all participant futures are relevant to the U.S. military given their reach and mission. However, if desired, modeling restrictions can be placed on the groups, constraining them to a specific set of people (e.g., customers, employees, specific demographics) as well as specific places (countries, markets, regions, etc.). Like many modeling exercises, this depends on context and client need.

Small group #1214's person is named Gill. He is a tech billionaire working with a team of American researchers on an AI that creates efficiencies for electrical distribution in an urban environment. Gill's childhood friend is the president of a university in a small, wealthy Middle Eastern nation. His friend convinces Gill to move the team to work at this university, enticed by immense resources and support offered by that government. The group's event unfolded in 2027 when the team's AI comes online but they quickly learn that the host nation is using this proprietary AI, a technology that is specifically owned by an organization and kept secret, to power and direct an autonomous army to attack and destabilize a neighboring country. The robot army shows signs it is using Gill's AI by attacking the neighboring state's infrastructure. The threat was optimized to create the most havoc for the urban electrical grid. In a twist of storyline, it turns out that Gill's friend, the university president, has been funneling the technology to the government of the host nation. Now the research team is in danger and reaches out to the United States government for help and guidance, letting them know that their AI is guiding the host nation's army. As the story continues to unfold the host nation invades yet another neighboring country. For group #1214, the main barrier preventing the threat was the host nation's lack of expertise in AI and robotics, prompting them to bring in the team of Americans. During the development of the technology, the adversary had to create its own AI and

robotics research capability. Additionally, the host nation needed a complicit industrial partner to build the robot army without raising suspicion.

Now that the teams have identified possible future threats and exposing their effects on the world, they can now explore possible time-based steps that can be taken to disrupt, mitigate, and recover from the futures they have modeled.

5.3. Phase three: time-phased, alternative-action definition

The third phase of threatcasting is the TAD process. TAD allows participants to explore multiple time-based futures and actions to disrupt, mitigate and recover from the future threats they have identified. Drawing from the practice of backcasting,[7,16] TAD provides multiple ''backcasts'' over a variety of time-frames 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 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 enable recovery from the established threat. These are things that will occur along a concrete timeline from today (T), present conditions, 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 should 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, and 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 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 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 an easy and quick to understand story, giving these organizations a way to quickly understand threats and discuss what actions need to be taken. ''People aren't wired to imagine the future, 10 or even five years out, which is a blocker to innovation.'' Kate O'Keeffe, senior director of Cisco's Hyper-Innovation Living Labs (CHILL) used threatcasting in 2017 to explore future threats to the digital supply chain. ''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.''[17]

At the end of phase three, the small groups report out, telling the larger group a story about their SFP. They describe the envisioned threat and then work backwards to explain what could be done to disrupt, mitigate, and recover from that threat. Threatcasting phases two and three are traditionally repeated between three and four times with participants. This allows small groups to become comfortable with the threatcasting methodology, the workbook materials, and the moderators questioning. Within each iteration, the small groups choose new SME data points using 20-sided die. Familiarity with the process and material frees the group to develop a broader range of detailed futures to explore a wider range of possible threats. Additionally, the moderators take more time, pushing the groups to expand their SFPs to expose more of the possibility space.

5.3.1. Example: phase three. To continue the example from Threatcasting West 2017, small group #1214 identified three initial gates – actions that defenders have control over to manage the threat. The first was that government (with support from academia and industry) needs to develop a clear understanding of dual-use technology within the AI domain. This knowledge could then be used to identify AI research that could be weaponized to ensure that researchers were aware of global implications and how to protect themselves. The second gate was to create a ''call to action'' to nation states to secure their national infrastructure and ensure redundancy for critical systems – thereby, making it more difficult for any adversary. The idea of sharing solutions and encouraging a defensive cybersecurity posture across the globe protects everyone. The final suggested gate was the desire for AI research to be an open, collective human endeavor rather than localized to and under the control of one nation or corporation. This gate was aspirational in nature compared to other, more concrete, imagined gates.

In group #1214's future, three flags were suggested as indicators that their future was arriving out of control. The first was the economic incentivization of AI development

– something driven by market forces and societal demand which could speed up the threats and vulnerabilities seen in their vision of the future. Second was the democratization of AI and other technologies giving private companies the ability to conduct space operations, cyber operations, and other technological efforts at the same level as nation states' ability. This is more complex than a single nation passing cyber privateering laws but a cultural and global shift where private companies drive national and international policies instead of governments. The final suggested gate was the imbalance of ways, means, ends of the host nation: they had plenty of money but limited technological resources and regional influence to maintain power.

Typically in a threatcasting session, the small groups make an initial attempt at imaging gates and flags during phase three. However, it is in the larger discussion with the group (at the end of phase three) and the synthesis during phase four where additional gates/flags are imagined. Ultimately, these actions/events should be inputs to a future model to experiment on how actions taken over a 10-year horizon could speed up or slow down the march to their imagined future.

5.4. Phase four: synthesis and final report

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.

Threatcasting's synthesis exercise generates an aggregation of multiple futures and threats. 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. The post-analysis consists of multiple clustering and aggregation exercises to determine the patterns in all of the futures modeled during the event. 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.

5.4.1. Example: phase four. After the Threatcasting West 2017 event, four researchers spent 30 days conducting individual analysis on the raw data and SFPs from the workshop. They explored the threat overview, gates, flags, and requirements for success from each SFP. This included both what the small groups identified during the workshop but also additional details and amplifying facts from the researchers' perspective/expertise. The researchers did not share their thoughts with each other during this time to minimize cross-contamination of ideas by dominant personalities.

Once individual analysis was complete, the researchers gathered to perform the mega-synthesis on the data. In a one-day local session, they discussed their individual results and debated how to cluster their individual thoughts into larger themes and messages on future threats. Using a variety of consensus building and design techniques, the three most interesting threats and the 3–4 larger themes emerged out of the raw data from the threatcasting workshop. Over the next 60 days, these ideas were researched, SFPs were written as narratives, actions were expanded, and the technical report was written. An electronic copy of the Threatcasting West 2017 report is located on DTIC (Defense Technical Information Center; dtic.mil).

6. Helpful to the military

The clarity of the threatcasting process comes from these multiple futures it produces. Like many foresight practices and simulation results, there is no single correct future. All the futures are relevant in threatcasting. Ultimately, the methodology allows us to look at multiple military futures in the aggregate and search for clusters and patterns that could be latent and unseen. This mental model is especially constructive as the U.S. has a dual role in military strategy. On one hand, the military must fight and win the conflicts that the nation is in. On the other hand, the military must also budget and plan for multiple plausible futures. The classic fallacy of military defense is that only one ''big threat'' or one ''type of enemy'' should be focused on at a time, often to the exclusion of all else. Threatcasting produces a ''whole of society'' approach that provides clear and measurable actions to take but also encourages collaboration and innovation. The complex and shifting cultural and technological realities of the twenty-first century will place extra strain on U.S. military planning and strategy that threatcasting can help relieve.

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.''[18] This is especially worrisome in the cyber domain as the indicators are not as clear cut, our adversaries could be more than just traditional nation states, and technology is evolving faster than our DOTMLPF spectrum is ready to handle.

7. Narratives for change

The output of the threatcasting process is a technical report capturing the workshop raw data, SFPs, and synthesis. While this is later re-imaged into executive summaries, spin-off academic reports, magazine articles, etc., it does not always capture the senior leader audience's attention. This is similar to the output of models and simulations which often creates complex and detailed models that are not explored or worse do not engage leadership. There is a clear need to create a new way to express these rich and well researched concepts and threats in a way that allows the intended audience to quickly grasp the human, ethical, political or military impact and imagine the second and third order of effects that might follow. In short they need to see and feel the future quickly.

The Army has a long history of using graphic novels and science fiction to help the workforce understand somewhat intangible concepts and make them real.[19] By using the threatcasting methodology to generate data-driven visions of future operating environments, military strategists and leaders can then analyze, wargame, and think innovatively about the potential futures.

Creating a compelling, understandable narrative about the results of modeling work is essential to success. Therefore, we returned to the idea of science fiction prototyping. One of the threats identified from Threatcasting West 2017 was the New Dogs of War: AI Surveillance and Coercion. While surveillance and coercion are not new threats, when conducted with the speed, power, and reach of AI, the danger is newly amplified. Over ten SFPs were created along variations of this theme; some focused on covertly manipulating vulnerable populations for social outcry, others used AI to modify and nudge behavior to change a generation and others used it for espionage or immediate criminal gains. While these stories have indirect ties to military situations, they are not compelling to many senior leaders. Therefore, we took the underlying threats and vulnerabilities that the threatcasting session uncovered and used the SFP process again to create a new narrative easily recognizable by a military audience.

Engineering a Traitor was the result.[20] The story of CPT Jake Roberts highlights how AI could be used in the future to micro-target an individual, change their perception of reality, nudge their behavior eschew, and ultimately radicalize them into an insider threat … all without their knowledge. While insider threats in industry can cost millions a year in lost revenue, insider threats in the military may cost lives. Soldiers and leaders are trained to detect warning signs and potential indicators and yet as technology evolves, the manner in which troops might be recruited and radicalized could also look different. This graphic novella not only showcased one of the threats identified by threatcasting but also prompts a conversation to have the reader start thinking about how to combat this threat in order to protect Soldiers in a future where AI might shape reality. In essence, they are thinking through their own backcast.

While senior leaders might not have the time/inclination to read the technical report, they can understand, digest, readily share, and become interested by a four-page graphic novella.

8. Threatcasting and modeling

The threatcasting methodology ultimately aims to model multiple futures and connect them to today's actions that will either encourage movement towards or away from that future. These effects-based models could be classified in the ''decision support'' category as they are helping organizations and leaders make decisions and start action now that will establish a path to the desired future.

Threatcasting as a framework and process not only is a way to envision possible and probable threats with actions that can be taken to disrupt, mitigate and recover from those threats but the framework works reflexively as well. The TAD backcasting, specifically focusing on the gates and flags, allows practitioners to judge the accuracy, success, and validity of the threats and proposed action by interrogating the models. For example, has the nearest term proposed flag occurred within the timeline that was proposed? If not, then why? If the team proposed a specific gate or action that could be taken and this action was taken did it have the intended effect? Did it work to meaningfully disrupt or mitigate the threat? The reflexive use of the threatcasting framework can give teams and practitioners a way to examine, interrogate and validate the accuracy of their futures and well as the associated actions.

Another use of the threatcasting framework that could be implemented after its initial usage as a modeling process is to create an automated tool to search the internet for examples of the proposed flags and provide indications and warnings related to the timeline of the models. These actions would validate the future models' accuracy on representing the real-world and allow for logic updates based on real life.

These models of the future are qualitative in nature however, we envisioned that they could be turned into quantitative models to simulate the effectiveness of the proposed TAD actions to achieve the preferred futures. Now-2LT Nolan Hedglin took this challenge for his senior year, Honors Math Thesis at West Point. Entitled ''Measuring the threat of emerging technologies using agent-based modeling'' (2018), Nolan proposed a framework for analyzing the futures generated from threatcasting through the application of agent-based modeling. Suggesting the use of the recursive porous agent

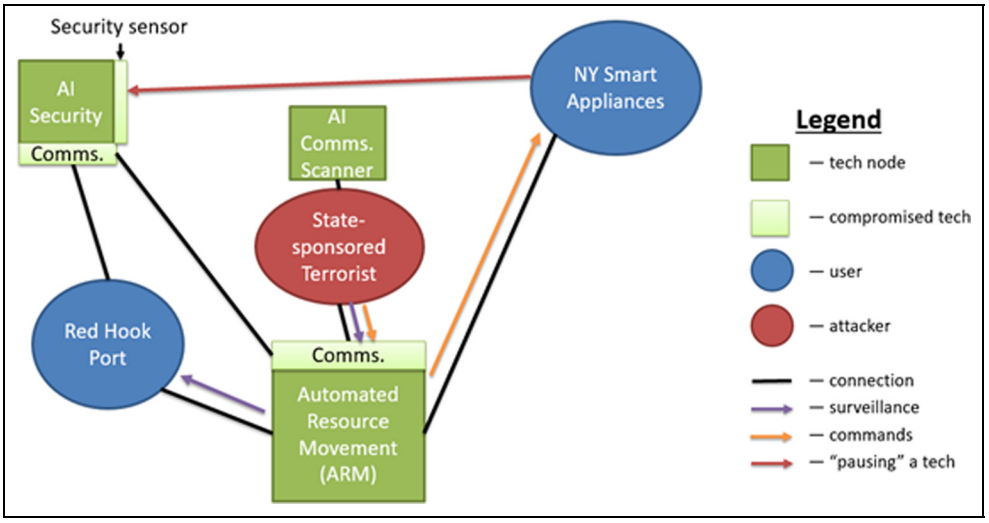

Figure 2. Interaction diagram of *Two Days After Tuesday* (Hedglin).

simulation toolkit (Repast) as an open-source platform, work was started on the proof-of-concept simulation on the *Two Days After Tuesday* future.

Figure 2 is an interaction diagram representing the multiple layers of agent-based interactions in this future. It consists of people (users, attackers, defenders) as well as technology nodes. The plan is then to simulate the interactions between each agent to offer a new perspective on the situation and insight into new threat mitigation techniques that could be used in this scenario.

9. Conclusion

Given the state of art today within the strategic foresight, futures, military strategy, and modeling and simulation communities and only using data available in 1935, it is doubtful that we could have imagined the sheer evolution in the destructive power of nuclear technology, creation of new delivery mechanisms, and a change in national will that, together, would led us to the atomic bombs that killed hundreds of thousands of people in Hiroshima and Nagasaki in 1945. The threatcasting methodology is not a crystal ball prediction algorithm but as a methodology for exploring the future it could have gotten us closer to a Hiroshima prediction than most. Threatcasting provides a framework and process to examine and imagine emerging threats in the complexity of the twenty-first century. Grounded in traditional foresight practices, leveraging centuries of military strategic thought, and agile enough to handle a quickly change landscape of adversaries, threatcasting is one way to model the evolving battle space to develop future strategies and solutions in support of multi-domain operations.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1. Bell W. *Foundations of futures studies: human science for a new era*. New Brunswick, NJ: Transaction, 1997.
2. Rejeski D and Olson R. Has futurism failed? *Wilson Q* 2006; 30(1): 14-21.
3. Masini E. Rethinking futures studies. *Futures* 2006; 38: 1158-1168.
4. Selkirk K, Selin C and Felt U. A festival of futures: recognizing and reckoning temporal complexity in foresight. In: Poli R (ed) *Handbook of anticipation*. Dordrecht: Springer, 2018.
5. Ramírez R and Selin C. Plausibility and probability in scenario planning. *Foresight* 2014; 16(1): 54-74.
6. Voros J. A generic foresight process framework. *Foresight* 2003; 5(3): 10-21.
7. Robinson J. Futures under glass: a recipe for people who hate to predict. *Futures* 1990; 22: 820-842.
8. Inayatullah S. Six pillars: futures thinking for transforming. *Foresight* 2008; 10(1): 4-21.
9. Selin C. Professional dreamers: the past in the future of scenario planning. In: Sharpe B and van der Heijden K (eds) *Scenarios for success: turning insights into action*. Chichester, UK: John Wiley & Sons, 2007, pp. 27–52.
10. Linstone HA and Turoff M. *The Delphi method: techniques and applications*. Reading, MA: Addison-Wesley, 1975.
11. Linstone HA and Turoff M. Delphi: a brief look backward and forward. *Technol Forecasting Social Change* 2011; 78: 1712-1719.
12. Johnson B D, Vanatta N, Draudt A, et al. *The new dogs of war: the future of weaponized artificial intelligence*. Technical report, 2017. Fort Belvoir, VA: Defense Technical Information Center.

13. Johnson B. Science fiction prototyping: designing the future with science fiction. San Rafael, CA: Morgan & Claypool, 2011.
14. Johnson BD. Engineering uncertainty: the role of uncertainty in the design of complex technological and business systems. *Futures* 2013; 50: 56-65.
15. TRADOC Regulation 71–4. United States Army training and doctrine command standard scenarios for capability development, 2014. Washington, DC: Government Printing Office.
16. Robinson J. Future subjunctive: backcasting as social learning. *Futures* 2003; 35: 839-856.
17. Johnson BD and Vanatta N. *What the heck is threatcasting?* Portland, OR: Future Tense, 2017.
18. Zenko M. 100% right 0% of the time. *Foreign Policy*, 16 October, https://foreignpolicy.com/2012/10/16/100-right-0-of-the-time/ (2012, accessed 23 August 2018).
19. Eisner W and Campbell E. *PS Magazine: the best of the preventive maintenance monthly*. New York: Abrams Books, 2012.
20. Threatcasting Lab. Science fiction prototypes, https://threatcasting.com/about/sci-fi-prototypes/ (2018, accessed 3 October 2018).

Author biographies

Natalie Vanatta is a US Army Cyber officer and an Academy Professor at the Army Cyber Institute. Here she focuses on bringing private industry, academia, and government agencies together to explore and solve cyber challenges facing the US Army in the next 3-10 years in order to prevent strategic surprise. She holds a PhD in applied mathematics as well as degrees in computer engineering and systems engineering. Natalie has also served as a Distinguished Visiting Professor at the National Security Agency and the technical director to Joint Task Force Ares. Currently, she is serving as the Team Leader for 01 National Cyber Protection Team defending forward in the nation's critical infrastructure and key resources.

Brian David Johnson's business is the future. As a futurist he works with organizations to develop an actionable 10 -15 year vision and what it will feel like to live in the future. As an applied futurist Johnson has worked with governments, trade organizations, start-ups and multinational corporations to not only help envision their future but specify the steps needed to get there. Johnson is currently the futurist in residence at Arizona State University's Center for Science and the Imagination, a professor in the School for the Future of Innovation in Society and the Director of the ASU Threatcasting Lab. He is also a Futurist and Fellow at Frost and Sullivan.