The Future of Weapons of Mass Destruction when Emerging Technologies Arise

COL Natalie Vanatta
Army Cyber Institute at West Point, NY
USA

natalie.e.vanatta.mil@army.mil

Brian David Johnson
Arizona State University, Tempe, AZ
USA

Keywords: Cognitive Superiority; Weapons of Mass Destruction; Emerging Disruptive Technologies; future threats; Threatcasting;

ABSTRACT

Technology today is rapidly evolving and quickly being adopted into our everyday lives. But what will the future hold? Not the science fiction future of space travel but the future in the next 5-10 years. How will individuals and communities embed this technology in their lives? How will our adversaries exploit the vulnerabilities that arise? How will the Alliance combat these threats, address the risks, and take advantage of the opportunities? How do we prepare for an increasingly complex and dangerous future?

Visualizing what this future will hold, and what new threat vectors could emerge, is a task that in the 21st century, traditional planning mechanisms have struggled to accomplish. Traditional planning processes struggle to comprehend the complexity and speed of a wide range of potential issues. Understanding and preparing for the future operating environment is the basis of an analytical method known as Threatcasting. Threatcasting uses inputs from social science, technical research, cultural history, economics, trends, expert interviews, and even a little science fiction to explore future threats and design potential futures.

On 01-02 March 2022, the Army Cyber Institute and NATO Allied Command Transformation convened a multi-disciplinary group to use the Threatcasting methodology to explore how future Emerging Disruptive Technologies might increase the effectiveness and lethality of Weapons of Mass Destruction in kinetic warfare. This paper will discuss the results of this project as well as identify specific actions, indicators and concrete steps that can be taken today to disrupt, mitigate and recover from these future threats.

1.0 INTRODUCTION

Technology today is rapidly evolving and quickly being adopted into our everyday lives. But what will the future hold? Not the science fiction future of space travel but the future in the next 10 years. What new technologies will move and change our lives? How will individuals and communities embed this technology in their lives? How will our adversaries exploit the vulnerabilities that arise? How will the Alliance combat these threats, address the risks, and take advantage of the opportunities? How do we prepare for an increasingly complex and dangerous future?

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

methodology assists and enables practitioners to imagine enemy innovations before they happen and identify actions that can disrupt or respond to these adversary 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 future events and trends (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 perils. The Threatcasting methodology also exposes what events could happen that indicate the progression towards an increasingly possible threat landscape.

The specific research question that this paper explores is: "*How might future Emerging Destructive Technologies (EDTs) increase the effectiveness and lethality of Weapons of Mass Destruction (WMDs) in kinetic warfare?*" Our hypothesis is that using the Threatcasting methodology on this research question will produce a range of possible and potential detailed threat futures at the intersection of WMDs and EDTs. These futures will provide readers and practitioners:

- A rich data set to understand the possible effects of EDTs on WMDs along with clear actions to be taken to disrupt, mitigate and recover from these effects.
- Specific indicators that one or more of the threat futures is beginning to manifest.

This work was done in conjunction with NATO Allied Command Transformation (ACT) Strategic Plans & Policy (SPP) branch, the Army Cyber Institute (ACI) at West Point, and Arizona State University (ASU).

1.1 Weapons of Mass Destruction (WMDs)

The United Nations refers to WMDs as a "class of weaponry with the potential to, in a single moment, kill millions of citizens, jeopardize the natural environment, and fundamentally alter the world and the lives of future generations through their catastrophic effects." [1] The United States Department of Defence, in Joint Publication 1-02, defines WMDs as "chemical, biological, radiological, or nuclear weapons capable of a high order of destruction or causing mass casualties." [2] More broadly, WMDs are weapons designed to both terrorize and deter. [3] The very idea of these weapons is itself "weaponizable," meaning the threat of deploying WMDs is often as effective as the weapons themselves — hence the vastly greater hesitation to use them. Images of poison gas, mushroom clouds, and horrific plagues are deliberate and effective enhancers of fear and confusion and great deterrents to avoid conflict escalation (as seen recently in the context of Ukraine).

1.2 Emerging Disruptive Technologies (EDTs)

As the acronym would indicate, EDTs are an umbrella term for a number of disparate technologies that are both emerging — from the laboratory stage to a step away from mass production — and disruptive, in that they pose challenges to existing doctrine for non-proliferation and deterrence. [4] Within the scope of this paper, EDTs possess outsized potential to 1) accelerate conflict escalation and lower the bar for the use of WMDs; 2) replicate and/or enhance the lethality and/or long-term destructiveness of WMDs when paired together or used in tandem, and 3) offer dual uses with defence and security applications as well as pose potential threats.

Different organizations define different sets of technologies to be designated as EDTs. NATO [5], the White House [6], the U.S. Army [7], Academia [8], and Forbes [9] have published their lists of EDTs just to name a few. While there exists some similarities, there also exist differences. For the purpose of answering this research question, we defined the following technologies as EDTs:

- Advanced Computing (including supercomputing, edge computing, new architectures, big data, and sentient data),
- Advanced manufacturing,
- Artificial Intelligence (including human-machine teaming),
- Autonomous Systems and Robotics,
- Biotechnologies (including synthetic biology, or "synbio"),
- Cyber,
- The Internet-of-Things (especially relating to government or municipal IOT for infrastructure),
- Hypersonics, and
- Quantum Information Technologies.

The challenge remains that many of these EDTs are dual use; namely, their development will result in both improvements within society but also can lead to their weaponization against that same society.

2.0 THREATCASTING OVERVIEW

The Futrecasting and Threatcasting Methodologies [10] are strategic foresight methodologies that have been routinely and successfully applied to industry [11] and national security problems [12], [13]. Threatcasting uses inputs from social science, technical research, cultural history, economics, trends, Subject Matter Expert (SME) 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. This methodology also exposes what events could happen that indicate the progression towards an increasingly possible threat landscape.

Several foresight and modelling methods are available to explore the future of WMDs and EDTs. However, the Threatcasting methodology has some unique attributes that set it apart from others. The methodology differs from traditional scenario planning in that it gives a higher degree of detail and multiple perspectives on the threat. Threatcasting utilizes some aspects of the Delphi method, however the final data and output from the workshop not only gathers consensus around possible and potential threats, as produced by the Delphi method, but it also documents specific actions and indicators that the Delphi method does not produce.

The advantages to the Threatcasting methodology are that it pulls from cross-disciplinary inputs (SME interviews) and utilizes a diverse set of participants to conduct a workshop which produces a robust and detailed data set for the analysts to do their findings. The U.S. Army has used the methodology on various national security problems for the last six years with success. To the best of the authors' knowledge, this is the first time this methodology has been applied to the field of WMDs.

2.1 Threatcasting Workshop Virginia Beach

On 01-02 March 2022, 60+ participants convened in Virginia Beach, Virginia to explore how emerging technologies might enhance the effectiveness and employment of weapons of mass destruction.

Utilizing the foundations of the Threatcasting methodology, the participants were curated to be diverse in experience, expertise, and outlook. The pool of participants included undergraduate students from all six

U.S. senior military colleges (Norwich University, Texas A&M University, The Citadel, Virginia Military Institute, Virginia Tech, and the University of North Georgia) and two U.S. service academies (United States Military Academy and United States Air Force Academy) as well as professors from colleges within the U.S. and Europe. It also included company grade officers from the U.S. Army and field grade officers from NATO countries. And last but not least, it included very talented researchers from National Labs as well as strategic thinkers from across Industry.

2.2 Phase 1

Phase 1 in the Threatcasting methodology is the research synthesis with the intent to capture the "wisdom of the room". [10] Unlike the Delphi method [14] – which engages expert opinion through iterative rounds of questioning and feedback – here, the insights of the participants (and how they react to the initial SMEs) are as important as the insights from the SMEs. The participants are presented with curated SME videos that address different perspectives/domains around the primary research question. These videos provide research, data, and expert opinions on the current state of their domain and how it might evolve over the next decade (as it pertains to the research question). Then, the iteration of these ideas comes from the participants instead. Unlike Delphi, the goal is not to reach a consensus on one idea, but to provide the unique data points that become the scenario framework and are, ultimately, integrated with the participants' insights and synthesis.

To accomplish this, the participants are first asked to identify all the key or salient points that the SMEs provided in their taped remarks that they felt would have some bearing on the research question. Once complete, the participants were organized into small working groups of 3-4 people to synthesize these inputs. Namely, they discussed and provided feedback on three open-ended questions for each key point:

- What are the implications of the data point on the research question?
- Are these implications positive or negative or neutral?
- What should we do about it?

The first question captures the participants bias, opinions, contradictions, and expertise. The second question gives further feedback on the key point and forces participants to think about it from different perspectives. The third and final question is meant to get the participants to start thinking about specific micro actions that could/should be taken in the future.

For the WMD + EDT research question, we used 8 SMEs to lay out the foundations of what 2040 might look like. The SMEs are listed below:

- **SME #1 - Dr Melanie Sisson**. [15] She is a fellow in the Brookings Foreign Policy program's Centre for Security, Strategy, and Technology where she researches the use of the armed forces in international politics, U.S. national security strategy, and military applications of emerging technologies. In her taped remarks to the participants, she introduced participants to the foundational concepts of nuclear deterrence and how EDTs will affect state's nuclear strategies.
- **SME #2 - Dr. John Arquilla.** [16] He is an emeritus professor at the Naval Postgraduate School; an expert in special operations, unconventional warfare, and international policy. In his taped remarks to the participants, he discussed: 1) the complexity of cyberspace, 2) how power and vulnerability go hand in hand, 3) defence versus prevention, 4) various EDTs, and 5) technological advances lowering the barriers to proliferation.
- **SME #3 - Sarah Gamberini.** [17] She is a Policy Fellow at the National Defense University (NDU) Center for the Study of Weapons of Mass Destruction (CSWMD). In her taped remarks to the participants, she discussed quantum sensing's potential impacts on strategic deterrence, modern warfare, and its implications for WMDs.

- **SME #4 - Dr. Genevieve Bell.** [18] She is a renowned anthropologist, technologist, and futurist. She is currently the Director of the School of Cybernetics and Florence Violet McKenzie Chair at the Australian National University (ANU), and a Vice President and Senior Fellow in Intel Labs at Intel Corporation. In her taped remarks to the participants, she discussed five threads out of the pandemic about human behaviour and engagement that might foreshadow the future world.
- **SME #5 - Dr. P.W. Singer.** [19] He is a Strategist at New America, a Professor of Practice at Arizona State University, and Founder & Managing Partner at Useful Fiction LLC. In his taped remarks to the participants, he discussed how "strategic surprise" is looking right at us. This included topics such as future roles of technology in both society and the military, talent management, trust, and our relationship with technology.
- **SME #6 - Col. Beth Markos.** She is a permanent professor at the United States Air Force Academy. She is also a command pilot with more than 2,000 hours of flight experience and has served as an Air Operations Centre Commander, Squadron Commander, and Instructor and Evaluator pilot in both the B-2 (nuclear capable bomber) and T-38. In her taped remarks to participants, she discussed the EDTs that would most impact nuclear operations and nuclear strategy.
- **SME #7 - Andrew Hessel.** [20] He is a micro-biologist, geneticist, and entrepreneur. In his taped remarks to the participants, he discussed how EDTs could enhance biological WMDs.
- **SME #8 – Representative from the United States Air Force Futures' Futures and Foresight Team**. In his taped remarks to the participants, he discussed elements of the 2022 Air Force Global Futures report as they pertain to the research question.

Given these initial SME insights, the participants developed 95 synthesized points they felt would have a bearing on the development of future operating environments.

2.3 Phases 2 and 3

Phase 2 in the Threatcasting methodology is the Futurecasting. [10] Here the participants, placed in those same small groups of 3-4 people, created their vision of 2040; where emerging technologies had affected weapons of mass destruction. This phase was designed as an effects-based model that used the data points from Phase 1 and integrated elements of participatory design [21], experience design [22], and the science fiction prototyping process [23].

These small groups pseudo-randomly selected data points from the research synthesis phase and used those as the foundation for their 2040 world. The intersection of the SME data points and the commentary around implications give the participants the needed raw inputs 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 physical or digital instantiation of the problem caused by the threat is then described as the 'event'. Participants explore the *event* from both the "blue" and "red" perspective. This is all done through a list of questions particularly designed to create a compelling narrative.

Phase 3 in the Threatcasting methodology is the Time-Phased, Alternative-Action Definition (TAD) process [10]. Using the threat future (effects-based model) that was created in Phase 2, the small groups next explore how to disrupt, mitigate, and recover from the threat. They will also identify the actions that can be taken and the indicators (flags) that will indicate the threat is beginning to manifest itself. The Threatcasting Method expands traditional backcasting [24] from looking at a single path to a specific threat future to a vision that explores multiple paths and possibilities.

Ultimately, the participants created 52 stories through four rounds of Phases 2 and 3. At each round, the groups selected a different combination of key points from the Research Synthesis workbook to create the foundation of their future world:

- Round 1 utilized a standard set of questions for participants to develop the model; the focus was for participants to get comfortable with the process.
- Round 2 was modified according to the models created in Round 1.In this second round, groups were required to select a single WMD and a single EDT that had to interact during their 'event'. These two required data points were also combined with a pseudo-random selection of the phase 1 data points to create the foundation of their scenario.
- In round 3 we added new restrictions to ensure we had a good coverage of the 3 WMD types and the 9 EDTs in the data set. Namely, the participants had to pick 1 WMD type (different than what they selected in round 2) and then 3 EDTs (but not quantum) to intersect during the 'event'. Then, we took a creative spin.
- In round 4, the groups were tasked with envisioning a future 'event' that did not use a traditional WMD. Instead, it was a combination of EDTs and potentially kinetic effects that created similar destructive components as we saw with the dropping of "Little Boy" on Hiroshima.

After the Virginia Beach workshop was completed, five analysts[1] came together to synthesize and analyse the data collected from the participants. This result in a set of findings related to the research question as well as specific actions and implications for the NATO alliance.

2.4 New Threats

These advances in technology expose a new threat landscape and seven general threat spaces emerged. The first three focused on the effects of EDTs on traditional WMDs. The second set focused on how a combination of EDTs could be deployed with traditional weapons to create a "WMD effect" without resorting to a traditional WMD use. The analysts then reviewed, processed, and examined the findings, consulted SMEs, and produced seven implications for NATO which can be found below:

2.4.1 Implication 1: NATO Should Widen the Nuclear "Firebreak" to Minimize Conflict Escalation

EDTs initiate, facilitate, and escalate existing geopolitical conflicts, increasing the risk of general conflict and the use of WMDs. This is because EDTs accelerate, complicate, and scramble the classical models of escalation and deterrence. RAND strategist Herman Kahn developed a 44-step escalation ladder [25] mapping the conditional shows of force, acts of violence, and confrontations leading to an "all-out" war. Crucial to Kahn's model is the importance of both *context* and *thresholds*. Successful de-escalation depends on opposing actors' mutual ability to perceive and interpret each other's motives and intentions — without which they risk runaway escalation. Relatedly, escalating crises never proceed smoothly or inevitably from one rung to the next, but are rather tripped up at critical thresholds that act as a deterrent of "firebreaks" on decision-making. [26] Much like a firebreak is used to slow down or prevent the rapid spread of a wild fire, these deterrents could serve the same function [27]. For example, during the Cold War and since, the use of WMDs acted as the ultimate "firebreak" which even the Korean War or Cuban Missile Crisis could not cross.

EDTs short-circuit Kahn's and similar models in several key aspects:

- They scramble contexts through the use of AI and other rapid detection- and decision-making technologies that may obfuscate or deliberately misread opposing plans and intentions.

[1] Analysts included: Brian David Johnson (Arizona State University), LTC Natalie Vanatta, (Army Cyber Institute and United States Military Academy), LTC Jason Brown (Army Cyber Institute and United States Military Academy), Greg Lindsay (Atlantic Council), and James Carrott (Cultural Historian)

- They can be used after the initial provocation for misdirection and misinformation, creating strategic ambiguity while running the risk of escalation through misattribution.
- These risks are amplified by non-state actors' enhanced capabilities — for them, EDTs potentially carry more "bang for the buck" than either WMDs or conventional weapons when it comes to effects versus cost-and-complexity.

Therefore, NATO should widen the nuclear firebreak or nuclear deterrence capabilities and minimize/slow the spiral of conflict escalation. In fire sciences, a firebreak is a purposefully carved zone of earth, bare of flammable vegetation that contains the effects of a wildfire. In rugged terrain and uncertain weather conditions, these firebreaks must be dug where firefighters can most effectively reach them, not where they are most convenient. Sometimes, the firebreaks prioritize saving some parts of the landscape over others.

The key to minimizing the impact of EDTs on WMD escalation is to counteract the forces of distortion[2] and compression[3] while encouraging the effects of illumination on the adversary's actions. This would provide NATO the opportunity to be a leader of defining human, technical, and hybrid human-AI teamed firebreaks in NC3 systems.

2.4.2 Implication 2: NATO Should Raise the Bar for the Intent to Use WMDs

One reason the nuclear WMD threshold hasn't been crossed since Nagasaki may be the "nuclear taboo" [28] — a normative stigma powerful enough to stay the hand of even the most rationalist strategist. Other WMDs carry their own burdens — too weak to prevent their use, but strong enough to incite condemnation and potentially outsized policy responses compared to similar effects from conventional weapons. EDTs carry no such stigma.

Not only does their usage risk facilitating and accelerating the crossing of escalation thresholds, but they also threaten to lower the bar for the deployment of WMDs, partly by expanding the pool of potential participants to include non-state actors and others who have never lived in the shadow of WMDs or ever had reason to consider the nuclear taboo.

For state actors, the risk is existentially the opposite — attacking with EDTs may insert a rung on the escalation ladder that finally surmounts the nuclear taboo. In such a case, the presence of EDTs (and potentially WMDs) on both sides might heighten tensions and lead to a situation in which one decides to either strike first or escalate using EDTs. This in turn runs the risk of the perpetrator being met or counter-attacked with overwhelming force, thus finding themselves with their "back up against the wall," with seemingly no other choice than to use a nuclear WMD.

In the future, EDTs can create a condition where the intent to use WMDs is heightened. Raising the bar maintains the "taboo" of WMD use as well as slows the spiral of escalation to WMD use, most importantly in the use of tactical nuclear weapons during military conflict situations. The concern is that the use of EDTs in the "attack plain" creates a psychological space to feel backed into a corner, such that they feel their only recourse to restoring a power balance with NATO is to use a nuclear response. As an active participant in recent conflicts in Iraq, Syria, and Afghanistan, NATO has witnessed first-hand how the future of EDT-enabled conflict is emerging. NATO could become a trusted voice in leading and participating in these types of discussions.

[2] Distortion is when adversaries interrupt data flows and stretch/pull the information landscape selectively to their advantage.

[3] Compression is when the speed of conflict forces decision making in shorter and shorter timelines.

2.4.3 Implication 3: Expand NATO's Understanding of Insider Threats and Motivations

EDTs will enable, embolden, and amplify both old and new insider threats. Beyond attacks from known state- and non-state actors, EDTs will also introduce new vulnerabilities and produce outsized effects from insider threats (e.g., extremists, criminals, unknowing participants, etc.) whose behaviour can only be detected and modelled with difficulty. EDTs will amplify their roles as vectors, enablers, and unwitting accomplices in an unpredictably exponential manner, propelling them to the global stage and enabling them to affect geopolitical dominos.

One might imagine them doubling as unsuspecting carriers of personalized synthetic bioweapons targeting world leaders or other persons-of-interest. [29] Or they could conceivably act as radicalized "lone wolves" abusing access to dual-use EDTs such as cyber or quantum. EDTs can also be used to create or augment insider threats themselves. Cyber- and AI manipulation ranging from hacked personal and financial information to deepfakes and other forms of social engineering will be applied to compromise the mental health and security of personnel with access to critical systems.

In the future, the increased speed, scope, scale, and impact of an attack from a single person is amplified with the use of single or combined EDTs. It will be possible for an individual to have an outsized effect on NATO members using EDTs. Additionally, in the future, the "unknowing" insider threat could become more dangerous as EDTs (such as AI, Industrial IOT, and autonomous systems) can perpetrate and enhance an insider-based attack. Finally, attempting to find these unknowing insiders will prove near-impossible as they will not be displaying traditional indicators and warning signs of their intent.

This presents a current-day opportunity for NATO to lead an effort to develop a clearly articulated strategy for monitoring and training around insider threats for all NATO members. This should be combined with the exploration of this new category of the unknowing insider threat - exploring how the speed, scope, and scale of EDTs could affect how a person becomes a carrier. This will also include training to inoculate a person against manipulation and systems that can monitor for this type of activity.

2.4.4 Implication 4: NATO Should Address Plausible Scenarios of EDTs Interacting with Each Other and with WMDs

One reason the nuclear taboo or firebreak exists is that even in the absence of further escalation, nuclear WMDs create effects that are different in kind as well as magnitude. The horrific spectacle of instantaneous destruction, mass death, and chaotic disruption (ranging from millennia of contamination to nuclear winter [30]); places WMDs in another category altogether. However, by pairing or combining multiple EDTs, such as robotics, AI and autonomous systems, quantum, and hypersonics, state and non-state actors can achieve the speed, scale, and destruction of WMDs without crossing the nuclear threshold. As noted above, this will simultaneously escalate and lower the bar for the actual use of WMDs.

While unlikely to replicate full scope of WMD effects in a single attack, novel pairings of EDTs will succeed in achieving both immediate shock-and-awe and long-term degradation of the target's strategic resources. For example, cyber and quantum weapons might be deployed against civilian energy or transportation infrastructure to instigate a local- or regional attack with global shocks. Examples include such attacks on Ukraine's power grid in 2015 and 2016 (and allegedly in 2022) [31], or conceivably hacking personal vehicles to create widespread collisions, chaos, and deaths. More subtle attacks on critical social systems, such as healthcare, agriculture, finance, industry, and politics will have less visibility, but potentially more profound effects over time.

It is necessary for NATO to understand the full extent of multiple EDTs interacting with each other to provide sufficient detection mechanisms, preparedness, resiliency, and changes to collective defence measures. This understanding also requires NATO to consider the dual-use effects of EDTs for their intended scientific, social, and business applications, while simultaneously being used for conflict.

Currently, most EDTs are being developed by private industry, especially in western democracies [32]. Apart from China and to a lesser extent Russia [33], who both have maintained significant state control over research and development, advances in EDTs will happen outside of the control of NATO and its members. Organizations such as NATO's Advisory Group on Emerging and Disruptive Technologies can lead responses to technology innovation that is driven largely by the private sector. In that vein, NATO should "Set out objectives for harnessing dual-use, multi-use technology developments – capitalising on already existing technology from other domains and driving the development of multi-use outputs." [34]

Finally, NATO should develop critical enabler processes to monitor the use of single and combined EDTs, setting metrics for the measurement of when that EDT or combination of EDTs has the possibility of producing a WMD effect. NATO has recently revealed plans to develop a formal program that develops emerging technologies in a cooperative manner [35]. This plan was conceptually approved in NATO's June 2021 Brussels Summit, and materialized in 2022 through the approval of the Defence Innovation Accelerator of the North Atlantic (DIANA). DIANA "is designed to harness new academic, commercial, and entrepreneurial start-up technology, test and develop it as potential defence capability, and connect it more quickly to military end-user operational requirements." [36] DIANA's concept of nearly 50 test centres and accelerator programs is an ideal place for NATO to iterate and consider the implications of EDTs as they affect strategic and operational requirements.

2.4.5 Implication 5: NATO should Measure and Stabilize Complex Systems

The initial shock and destruction of combined EDT attacks will be accompanied by more pervasive and insidious efforts to achieve the long-term degradation of the opponent's strategic resources and capabilities. In turn, reducing its will and capacity to fight. The primary targets of these incursions will be the complex and interdependent systems undergirding nations and the international rules-based order: energy and infrastructure; healthcare; agriculture and food production; trade and the financial system; industry and raw materials; and other institutions whose health is essential to a functioning society.

The second- and third-order effects of these repeated attacks will be an erosion of trust in the affected systems and institutions, with the ability to create crises, unrest, and strategic paralysis. In the absence of an antagonist through an explicit attack with WMDs, the effects of these EDTs will be internalized, politicized, and increasingly intractable amidst domestic disputes. Breakdowns of social systems will manifest unpredictably through public disorder, infrastructure failures, domestic terrorism, and eventually large-scale effects that will present themselves as collapsing birth rates, rising deaths, and a steady decline in life expectancy.

The destabilization of one or more aspects of critical infrastructure is what can produce the destabilizing and lethal WMD effect(s) without the actual use of a WMD. Therefore, to monitor, disrupt, or mitigate this kind of threat, it is important to have a functional definition of what these complex systems or critical infrastructure might be. In the U.S., Presidential Policy Directive/PPD-21 identifies 16 critical infrastructure sectors [37]. The European Union has a similar definition but identifies 11 sectors [38]. NATO does not have an agreed upon definition of critical infrastructure, but it has encouraged research in the field [39]. It has also reinvigorated the efforts of "civil preparedness" that took a reduction in priority following the end of the Cold War. Resilience, as a national and collective value, is closely tied to the protection of critical infrastructure and to the tenets of Article 3 in the NATO Treaty; the seven baseline requirements for civil preparedness are outlined in the 2016 Warsaw Summit. [40]

NATO has the opportunity to establish a working definition of complex systems and critical infrastructure for members. This includes setting standards for measuring levels of contribution to NATO-wide civil preparedness and measurements to identify and describe emerging threats due to EDTs. NATO clearly understands the involvement that the European Union has in administering the critical infrastructure architectures and the relationship with the commercial sector. However, mechanisms and procedures need to be determined for testing how the civil sector and NATO should cooperate during a real event are lacking.

2.4.6 Implication 6: NATO Should Develop a Solutions Mindset for Long-term Potential Attacks

The greatest threat posed by EDTs compared to WMDs is their imperceptibility. Through the creative, deliberate, and patient use of EDTs in varying combinations to attack, destabilize, and persistently undermine critical systems, political will, and social cohesion, opponents might achieve the strategic effects of a WMD without their target's population even being aware they were the victims of an attack.

In addition to economic inequality, political polarization, and social mistrust, EDTs might also be employed to explicitly attack entire populations without detection. The COVID-19 pandemic has underscored how even a virus with a low positivity and deathrate has the propensity to trigger global upheaval. This is seen through broken supply chains, closed borders, and a long-term public health crisis. Future advances in virology and genetics raise the possibility of deliberately infecting or debilitating populations over years if not decades – to include indirect effects in rising healthcare costs, declining productivity, skewed dependency ratios, and other phenomena with dire consequences.

Another domain of concern is agriculture and the environment, which are both currently under stress in the West due to climate change. The global struggle by the U.S., China, and regional powers to secure a global food supply has already produced allegations of agricultural espionage, intellectual property theft, and genetic tampering. For example, imagine a modified virus attacks wheat or soybeans rather than human beings, which would trigger crop blights, soaring food prices, and societal breakdown. This could, with relative ease, be fuelled by information EDTs.

The implications are sobering. EDTs may simulate the effects of WMDs (i.e., EDTs may have impact on the order of magnitude of a WMD but spread over a longer period of time) without detection, and unlike the detonation of a nuclear missile above a city, society itself might be the attack surface.

With the current definition of WMDs and WMD effects, there is no exploration or specific framework for how a long-game attack might present itself. Because these attacks are designed to remain "under the radar", they will present themselves as criminal attacks, glitches in the system, or may remain hidden completely until their effects cannot be reversed.

The further development of EDTs by private industry will increase the hidden nature of their development. Additionally, because these EDTs will come out of industry, any attack or early indicator of an attack will present itself as a private sector crime or anomaly. NATO members may not even know that they are under attack from an adversary.

There is a risk, when sensing for the long-game attack, that a NATO member could be seen as monitoring noise or even being overzealous. For example, in April 2022, social media users seized upon a seemingly suspicious number of fires at food processing plants around the United States, leading media personalities, such as Turning Point USA founder, Charlie Kirk, to declare on Twitter, "Our food supply is under attack — the question is, by who?" [41] In fact, the fires were determined to be accidental and not statistically anomalous. [42] The point is that these facts did not deter social media users from continuing to push for an investigation.

NATO has an opportunity to work with members and their critical infrastructure and industry partners to begin sensing and measuring potential impacts in "grey space". Along with this sensing, a metric can be established to indicate when the activity being observed has moved from private sector crimes or anomalies to an EDT attack. Typically, this type of attack can be measured by its destabilizing effect on critical infrastructure.

2.4.7 Implication 7: Interaction with Non-Nation States and Corporations

The access to and increased effectiveness of future EDTs will allow non-traditional adversaries to attack NATO members. These adversaries will include non-nation state groups as well as corporations.

The current international framework of a state-based system is based on a system that was originally European in design. The state is a modern political construction that, in large part, grew out of the experience of European conflicts like the Thirty Years War but has evolved over the past centuries. A nation-state, then, is a system of order that expresses power over both borders and peoples. It follows then, that a nation-state would have all of the following: territory/space, bureaucracy/administration, control of the use of force/sovereignty, and a people or peoples (i.e., the dictionary idea of a "common descent, language, or history").

Today's digital world complicates the idea of territory/space. Our current ideas of territory and space are changing as we absorb the implications of cyberspace--in terms of how we conceive of and use physical as well as virtual artifacts to define them. Struggle over control of land has been a defining characteristic of the modern era (15th-20th century). In the new era we're living in, different struggles may assume the position of physical territory.

The modern global corporation was born in this context of the "frontier". Corporations have always functioned in hybrid environments, and there is quite a bit more to be considered with commercial organizations than a simple capitalist endeavour. Corporations exercise nation state powers more often than most people would think possible.

NATO must recognize that future allies and adversaries won't necessarily be constrained to nation states. Therefore, their model of partnership and membership along with their theories of deterrence will need to evolve.

2.5 Flags

The Threatcasting methodology not only maps possible and potential threats 10 years in the future but attempts to identify the flags (indicators) that serve as signals or trends indicating a specific threat future is underway. Sometimes referred to as "signals," these flags can give an early warning that a possible and potential threat future is in-flight or beginning to form. Often, flags are sequential with less apparent precursors already in effect, and the more alarming flags still over the horizon.

The data from the workshop provided three clustered groupings of indicators or flags that will signal the progression and development of EDTs. These groupings are relevant and apply to all 7 of the findings.

- **EDT Technical Progresses and Break Throughs**: Observing the progress and potential technological break throughs for EDTs is the primary landscape for any organization to monitor. The indicators will occur in multiple areas including academic research, private industry and corporate research and product offerings as well as nation state and military research. Spending resources to monitor the EDT landscape make it possible to identify key changes and influences in the development cycle that could disrupt, slow down or hasten the deployment of the EDT.
- **Geopolitical, Cultural and Business Trends**: Beyond the monitoring of the technological progress of EDTs, the threat futures depend heavily on the conditions into which the EDTs are deployed to increase the lethality of WMDs or produce WMD-like effects. The conditions or trends will span geopolitical, cultural, and business applications. An organization monitoring these indicators will improve their visibility about regarding developing conditions that contribute to the increased probability and susceptibility to threat futures. These are called out as three separate areas (geo-political, cultural, and industry) as the places and people that will need to be monitored are different.

- **Early Use, Rehearsals and Attacks:** The final grouping of indicators combines EDT technological progress and breakthroughs with the geopolitical, cultural, and business trends that set the conditions for WMD effects. This grouping of indicators illustrates a ramping up of severity over time. Early use does not necessarily indicate adversarial action, but simply the adoption of technology or any of the practices above that improve the conditions for an adversary's advantage. Rehearsals are generally tests that take place to prove out a strategy, to show a technology can achieve a specific effect, or to show others that an attack is possible. Early attacks are the final step in the indicators.

2.6 NATO Warfighting Capstone Concept

The NATO Warfighting Capstone Concept (NWCC) is a conceptual vision on how NATO members' militaries can gain and maintain advantage for the next twenty years. To achieve success, the military instrument must be able to Out-Think, Out-Excel, Out-Fight, Out-Pace, Out-Partner, and Out-Last the adversaries. [43]

These six "Outs" framed our analysis/synthesis on the participants' visions for NATO's actions, investments, and responses to be able to confront and defeat adversarial uses of EDTs and WMDs. Part of Phase 3 in the Threatcasting Methodology challenged our participants to determine actionable steps that could be taken to disrupt, mitigate, and/or recover from their threat future. The explanation of the Out is below however, the detailed list of actions can be found in the technical report [44].

2.6.1 Out-Think the Adversary

A key component to out-think the adversary requires that NATO members must have correct information. NATO's mutually trained intelligence processes are critical for gathering and understanding the vast amounts of data, information, and processed intelligence needed to out-think the adversary. Our data suggests this understanding arrives from several mutually reinforcing activities, including exploratory basic and applied research, detection and sensing, data sharing, and anticipatory decision-making informed by wargames at the individual country level.

2.6.2 Out-Excel the Adversary

Achieving excellence depends in part on understanding adversaries' motivations and capabilities; investing in the training, expertise, and tools necessary to counter potential threats, and developing shared infrastructure and capabilities to guide and regulate the evolution of these technologies. Our data suggests that these actions can be categorized as basic research & development (R&D), training and best practices, and purchases and investments.

As EDTs evolve beyond working proof-of-concepts and prototypes, NATO and its members must be prepared to develop, manufacture, operate, and regulate these technologies at scale. This requires building the necessary skills, supply chain, production capabilities, and training as well as the legal and policy frameworks needed to ensure responsible use and avoid proliferation.

This in turn will require NATO and its members to invest accordingly in new training and skills to instil these best practices at every level of the alliance. Doing so demands the creation of new facilities, centres of excellence, and tools to prepare NATO staff to meet these challenges. Finally, as EDTs reach maturity, NATO must invest in both guiding their development as well as creating safeguards against threats from adversaries, non-traditional actors, and insider threats.

2.6.3 Out-Fight the Adversary

In order for NATO to out-fight the adversarial use of EDTs, doctrinal, operational, and strategic changes to both deterrence and preparing for conflict are necessary.

EDTs' ability to simultaneously escalate conflicts while lowering the bar for WMD use creates a new level of complexity when capabilities are massed. This scenario could rapidly escalate through the overwhelming creation of multiple dilemmas (both in frequency and magnitude) which, in turn, will elevate multiple complexity into multiple wicked problems; ultimately resulting in decision paralysis. Additionally, non-nation-state actors armed with EDTs are potentially beyond the scope and capabilities of a traditional military alliance. Tomorrow's fights will not look like what is described in the history books. NATO has to be prepared to re-think the "sacred cows" and traditional thinking, to be prepared to defeat future adversaries.

Additionally, NATO needs to conduct activities that legitimize EDTs as a distinct category of threats and then incorporate them into updated models of deterrence. This includes developing new training and best practices for incorporating EDTs into organizations/units/entities.

2.6.4 Out-Pace the Adversary

How can NATO and its members out-pace the adversary, using new policies, processes, and technology to minimize the risks of WMD use and disrupt the adversary's decision-making process (OODA loop [45]) in an EDT environment? This will not only require pre-emptive regulation and restrictions on EDTs, but also rethinking logistics, communications, and planning to adapt in the face of new- and emerging threats.

Decades of nuclear arms reduction- and non-proliferation treaties, coupled with international monitoring efforts and national restrictions on the export of dual-use technologies have all been instrumental to reducing the risks of WMDs. A new generation of EDTs will require similar policies, and institutions to regulate dual-use technologies, such as robotics and AI, while restricting EDTs and WMDs, such as the biological agents capable of being paired with EDTs to create WMD effects.

Given EDTs' potential to rapidly escalate conflicts and create long-game WMD effects through attacks on infrastructure, it is incumbent on NATO to redesign its communication and supply lines to accelerate its responses to threats. NATO must expand and tighten communications between members, traditional partners, and new partners to match the sheer speed and disruption posed by EDTs. It must also reconceive "resilience" as a proactive capability in terms of how quickly NATO can meet and mitigate new threats, rather than simply have the capacity to recover from them.

2.6.5 Out-Partner the Adversary

Given the potential for the new categories of adversaries that we expect to see in the future, this means that the array of partners needed will also change.

Wargaming and joint exercises have been essential tools for NATO cooperation and cohesion since the alliance's formation. In this spirit, NATO should not only update its wargaming and planning playbooks to account for the special characteristics of EDTs, but also as a means to engage with new partners at different scales (e.g., international, national, local), different disciplines (e.g., technological and biogenetic), and different sectors (e.g., governments, NGOs, private sector).

As a political counterpart to wargaming and military exercises, NATO and its diplomatic arms should strategize how best to build support outside the alliance for the types of regulation and restrictions needed for monitoring, deterring, and interdicting EDTs.

Finally, given the scope of both potential actors and potential targets for EDTs, it's necessary to cultivate a whole-of-alliance and whole-of-society response to mitigating these threats. This will require closer coordination between NATO members' militaries, governments, and civil society, with the goal of forging a social consensus around the risks of EDTs in conflict escalation.

2.6.6 Out-Last the Adversary

In order to achieve and maintain a long-term perspective on potential threats and cultivate a culture of resiliency in response, NATO has to invest in education and people. This will enable its members to out-last the adversary.

Many of the technologies under the heading of EDTs, including robotics, AI, and biogenetics; are already at the centre of conversations around the future of talent, jobs, and economic growth. Building an alliance capable of meeting the threats posed by EDTs will require cultivating a workforce and a talent pool equal to the challenge of developing and/or combatting them.

Perhaps the best preventative measure against future EDT attacks by non-traditional actors and insider threats is to turn potential adversaries into allies in the present. NATO and alliance members should do this through investing in people, which not only means developing talent, but also resolving conflicts, reaching out to marginalized communities, and eliminating the conditions that foster radicalization.

Finally, resiliency (not only of our populations but also of our critical infrastructure) will be critical to out-lasting the adversaries. Developing programs and processes ensuring redundancy of essential services and infrastructure and the development of a society-wide will to fight through difficult and uncertain circumstances is key. Recent examples, like Russia's aggression in Ukraine, have shown the immediacy and importance of a country's preparedness and reliance on resilience.

3.0 SCIENCE FICTION PROTOTYPES

The data from the Threatcasting lab was not only used to write a technical report but will also serve as the scientific basis for two graphic novellas to be released in the late Fall of 2022. One will show how EDTs will accelerate conflict escalation among countries and lead to the increased use of WMDs. The second will illustrate how combined EDTs could be used by an adversary to produce WMD effects without the actual use of traditional WMDs. The purpose of these graphic novellas is to provide audiences a visceral and high-level overview of the possible and potential threats generated through the Threatcasting project. These science fiction stories are based on science fact but use narrative to convey the results a fresh and engaging way.

The United States Army has a long history of using visualizations to convey complex ideas. After WWI they had renowned comic book artist Will Eisner create *PS, The Preventative Maintenance Monthly.* This monthly magazine used illustrations and comic book art to convey technical information to soldiers about preventative maintenance techniques. [46] Carrying on the spirit of this approach, starting in 2017, the Army Cyber Institute released a series of graphic novellas (Dark Hammer [47], Invisible Force [48]) to investigate and explore future cyber and information warfare threats to the military.

4.0 IMPACT

The impact of this research will provide NATO and its members with a new, long-range perspective on the future of WMDs and EDTs. The results give detailed models for a range of possible and potential futures that currently are not in discussion and consideration as emerging threats. These threat futures will provide NATO a communication tool to explain and explore awareness and preparedness inside the organization itself as well as members.

This research also has exposed coming blind spots and areas for concern that not only on NATO's radar but by the very nature of the organization the threat would not be seen at all. This impact allows NATO to better prepare and develop a higher level of resilience to EDTs and WMDs.

Ultimately, the impact of the research provides NATO and members a specific roadmap to track the development of these threats as well as suggestions for possible actions that are tied specifically to existing NWCC planning and strategies.

The NWCC provides the Alliance a twenty-year perspective to maintain superiority in an ever-changing operational environment while conducting multi-domain operations. To implement this concept, NATO ACT created the Warfare Development Agenda (WDA) focused on five imperatives. The WDA will be executed in five-year planning increments along with the focus on "Jump Starters". The continued use of the Threatcasting methodology will provide a shared framework and research parameters over the successive planning periods but it will also all for the identification of new or variants threats related to previous NWCC activities.

5.0 CONCLUSION

The results of the Threatcasting project provided NATO with a broader range of possible and potential threats and specific actions to be taken at the intersection of WMDs and EDTs. Building off the initial objective and hypothesis, each of these new threats provided a high level of detail around the description of the threat, the 2nd and 3rd order effects, and how the threat might be identified. The data also provided specific implications to NATO and members both broadly and specifically applied to the NWCC.

To combat these future threats, NATO will need to conduct research and intelligence gathering paired with exploratory research and development to better understand the state of EDTs and their potential impacts. With this information, the Alliance will need to conduct collaborative "wargaming" and planning to explore a range of possible and potential threats of EDTs. The knowledge gained from all of these activities will inform future training and best practices to prepare for and address these threats.

NATO members and partners will also need to increase their investments in EDT related domains, necessitating countries to not only change how they fight, but also evolve their thinking about deterrence. Expanded regulation, policy making and political solidarity among members will take on an increasingly more significant and expanded role. Broader government, military, and civilian cooperation will be needed to disrupt and mitigate some of these future threats in conjunction with broader public awareness. All of these actions will place a higher value on cooperation and shared resiliency among NATO members.

6.0 ACKNOWLEDGEMENTS

The other analysts on this project were LTC Jason Brown, PhD (U.S. Army) and Greg Lindsey. Amazing thanks to our cultural historian Jaime Carrot. Finally, thanks to all our participants from across the globe.

7.0 REFERENCES

[1] "Weapons of Mass Destruction," [Online]. Available: https://unrcpd.org/wmd/. [Accessed 20 June 2022].

[2] U. Government, "Department of Defense Dictionary of Military and Associated Terms," [Online]. Available: https://irp.fas.org/doddir/dod/jp1_02.pdf [Accessed 20 June 2022].

[3] G. B. Roberts, "Hostis Humani Generis: The Threat of WMD Terrorism and How NATO is Facing the Ultimate Threat," *Defense Against Terrorism Review,* vol. 2, no. 1, pp. 1-13, 2009.

[4] NATO Science & Technology Organization, "Science & Technology Trends 2020-2040," NATO STO, 2020.

[5] NATO, "Emerging and disruptive technologies," [Online]. Available: https://www.nato.int/cps/en/natohq/topics_184303.htm [Accessed 20 June 2022].

[6] U. Government, "Technologies for American Innovation and National Security," [Online]. Available: https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security/ [Accessed 20 June 2022].

[7] U. Government, "Potential Game Changers," [Online]. Available: https://madsciblog.tradoc.army.mil/52-potential-game-changers/ [Accessed 20 June 2022].

[8] L. Munan, A. Porter and A. Suominen, "Insights into relatinoships between disruptive technology/innovation and emerging technology: A bibliometric perspective," *Technological Forecasting and Social Change,* vol. 129, pp. 285-296, 2018.

[9] F. T. Council, "15 Technologies That Will Disrupt The Industry in The Next Five Years," [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2020/05/07/15-technologies-that-will-disrupt-the-industry-in-the-next-five-years/?sh=58dc5f521239 [Accessed 20 June 2022].

[10] B. D. Johnson, N. Vanatta and C. Coon, Threatcasting, Morgan & Claypool, 2021.

[11] G. Hemingway and J. Loehr, "The Rock Factory," *Mining Magazine,* pp. 14-15, 2014.

[12] R. Lee, "Threatcasting," *IEEE Computer,* vol. 46, no. 10, pp. 94-95, 2016.

[13] N. Vanatta and B. D. Johnson, "Threatcasting: a Framework and Process to Model Future Operating Environments," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology,* vol. 16, no. 1, pp. 79-88, 2019.

[14] H. Linstone and M. Turoff, The Delphi Method: Techniques and Applications, Reading, Mass: Addison-Wesley Pub Co, 1975.

[15] "Melanie W. Sisson," Brookings, [Online]. Available: https://www.brookings.edu/experts/melanie-w-sisson/ [Accessed 20 June 2022].

[16] "John Arquilla," [Online]. Available: https://en.wikipedia.org/wiki/John_Arquilla [Accessed 20 June 2022].

[17] "Sarah Gamberini," [Online]. Available: https://wmdcenter.ndu.edu/Media/Biographies/Bio-View/Article/1621691/sarah-gamberini/ [Accessed 20 June 2022].

[18] "Genevieve Bell," [Online]. Available: https://en.wikipedia.org/wiki/Genevieve_Bell [Accessed 20 June 2022].

[19] "P.W. Singer," [Online]. Available: https://www.pwsinger.com/biography/ [Accessed 20 June 2022].

[20] "Andrew Hessel," [Online]. Available: https://en.wikipedia.org/wiki/Andrew_Hessel [Accessed 20 June 2022].

[21] T. Robertson and J. Simonsen, "Challenges and Opportunities in Contemporary Participatory Design," *Design Issues,* vol. 28, no. 3, pp. 3-9, 2012.

[22] F. Karray, M. Alemzadeh, J. Abou Saleh and M. N. Arab, "Human-computer interaction: Overview on State of the Art," *International Journal on Smart Sensing and Intelligent Systems,* vol. 1, no. 1, pp. 137-159, 2008.

[23] B. D. Johnson, Science Fiction Prototyping: Designing the Future with Science Fiction, Morgan & Claypool, 2011.

[24] J. Robinson, "Energy backcasting: A proposed method of policy analysis," *Energy Policy,* vol. 10, no. 4, pp. 337-344, 1982.

[25] H. Kahn, On Escalation: Metaphors and Scenarios (rev. ed.), Baltimore: Penguin Books, 1965.

[26] S. Kreps and J. Schneider, "Escalation firebreaks in cyber, conventional, and nuclear domains: moving beyond effects-based logics," *Journal of Cybersecurity,* vol. 5, no. 1, pp. 1-11, 2019.

[27] NATO, "NATO's nuclear deterrence policy and forces," 06 July 2022. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_50068.htm?selectedLocale=en [Accessed 01 October 2022].

[28] N. Tannenwald, "The Nuclear Taboo: The United States and the Normative Basis of Nuclear Non-Use," *International Organization,* vol. 53, no. 3, pp. 433-468, 1999.

[29] A. Hessel, M. Goodman and S. Kotler, "Hacking the President's DNA," *The Atlantic,* November 2012.

[30] A. Robock and e. al., "Climatic consequences of regional nuclear conflicts," *Atmospheric Chemistry and Physics,* vol. 7, no. 8, pp. 2003-2012, 2007.

[31] "Ukarine Russian Cyberattack," *The New York Times,* 12 April 2022.

[32] J. Thomas, "An Overview of Emerging Disruptive Technologies and Key Issues," *Development,* vol. 62, no. 1, pp. 5-12, 2019.

[33] C.-C. Hang, J. Chen and A. Subramian, "Developing Disruptive Products for Emerging Economies: Lessons from Asian Cases," *Research-Technology Management,* vol. 53, no. 4, pp. 21-26, 2010.

[34] NATO Advisory Group on Emerging and Disruptive Technologies, "Annual Report 2020," 2020.

[35] NATO, "NATO Sharpens Technological Edge with Innovation Initiatives," 07 April 2002. [Online]. Available: https://www.nato.int/cps/en/natohq/news_194587.htm [Accessed 02 October 2020].

[36] L. Willett, "NATO details DIANA technology programme," *Janes,* 11 April 2022.

[37] United States, White House, *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience,* 2013.

[38] SPEAR Project, "A Review of Critical Infrastructure Domains in Europe," 3 March 2021. [Online]. Available: https://www.spear2020.eu/News/Details?id=120 [Accessed 25 June 2022].

[39] NATO, "Critical Infrastructure Protection," 15 May 2020. [Online]. Available: https://www.nato.int/cps/en/natohq/topics_168104.htm?selectedLocale=en [Accessed 01 October 2022].

[40] Civil-Military Cooperation Centre of Excellence, "Resilience through Civil Preparedness: A CCOE Info Sheet," [Online]. Available: https://www.cimic-coe.org/resources/fact-sheets/resilience-through-civil-preparedness.pdf [Accessed 25 June 2022].

[41] C. Kirk, "Twitter," [Online]. Available: https://twitter.com/charliekirk11/status/1520171930325643266?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1520171930325643266%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Farticle%2Ffactcheck-processing-fire-idUSL2N2WW2CY [Accessed 20 June 2022].

[42] Reuters Fact Check, "Fact Check-Food processing plant fires in 2022 are not part of a conspiracy to trigger U.S. food shortages," [Online]. Available: https://www.reuters.com/article/factcheck-processing-fire-idUSL2N2WW2CY [Accessed 20 June 2022].

[43] NATO, "NATO Warfighting Capstone Concept," [Online]. Available: www.act.nato.int/nwcc [Accessed 20 June 2022].

[44] B. D. Johnson, N. Vanatta, J. Brown, G. Lindsay and J. Carrott, "Future Implications of Emerging Disruptive Technologies on Weapons of Mass Destruction," 2022. [Online]. Available: https://cyber.army.mil/Work-Areas/Threatcasting/ [Accessed 01 October 2022].

[45] W. S. Angerman, "Coming Full Circle with Boyd's OODA Loop Ideas: An Analysis of Innovation Diffusion and Evolution," AFIT, 2004.

[46] U.S. Army, "PS Magazine," [Online]. Available: https://www.psmagazine.army.mil/ [Accessed 20 June 2022].

[47] Arizona State University, "DARK HAMMER: A Retrospective of Science Fiction Prototyping," [Online]. Available: https://threatcasting.asu.edu/Dark_Hammer_Retrospective [Accessed 20 June 2022].

[48] Arizona State University, "INVISIBLE FORCE: Information Warfare and the Future of Conflict," [Online]. Available: https://threatcasting.asu.edu/invisibleforce [Accessed 25 June 2022].