INFORMATION WARFARE AND THE FUTURE OF CONFLICT

A Threatcasting Lab Report

INFORMATION WARFARE AND THE FUTURE OF CONFLICT

Technical Report by
Brian David Johnson, Alida Draudt, Jason C. Brown, Lieutenant Colonel Robert J. Ross, Ph.D.

From 2019 Threatcasting Workshop hosted at Arizona State University
produced by Cyndi Coon.

The Threatcasting Lab is supported by

ALL WATCHED OVER BY MACHINES OF LOVING GRACE

By Richard Brautigan 1967

I like to think
(and the sooner the better!)

of a cybernetic meadow
where mammals and computers
live together
in mutually programming harmony
like pure water touching clear sky.

I like to think
(right now, please!)

of a cybernetic forest
filled with pines and electronics
where deer stroll peacefully
past computers
as if they were flowers with spinning blossoms.

I like to think
(it has to be!)

of a cybernetic ecology
where we are free of our labors
and joined back to nature,
returned to our mammal brothers and sisters,
and all watched over
by machines of loving grace.

TABLE OF CONTENTS

PARTICIPANTS

A. David Abitbol, Ph.D.	U.S. Army War College
Andrew G. Clayton	Wieden+Kennedy
Major Jessica Dawson, Ph.D.	Army Cyber Institute
John B. Edwards	United States Secret Service
Renny Gleeson	Wieden+Kennedy
Colonel Andrew O. Hall, Ph.D.	Army Cyber Institute
Maxim Kovalsky	Army Reserve Cyber Protection Brigade
Steven Latino	ASURE
Ryan Manness	Naval Postgraduate School
Alycia de Mesa	ASU School of Sustainability, School for the Future of Innovation in Society
Lieutenant Colonel Robert J. Ross, Ph.D.	Army Cyber Institute
Bryan Sparling	U.S. Army Cyber Command
Anonymous	

ASU THREATCASTING LAB TEAM

Brian David Johnson	Director
Cyndi Coon	Chief of Staff
Natalie Vanatta	Senior Advisor to the Lab
Jason Brown	Ph.D. Student

Arizona State University Threatcasting lab

The Threatcasting Lab at Arizona State University serves as the premier resource for strategic insight, teaching materials, and exceptional subject matter expertise on Threatcasting, envisioning possible threats ten years in the future. The lab provides a wide range of organizations and institutions actionable models to not only comprehend these possible futures but to a means to identify, track, disrupt, mitigate and recover from them as well. Its reports, programming and materials will bridge gaps, and prompt information exchange and learning across the military, academia, industrial, and governmental communities.

THE FUTURE OF CONFLICT

In the coming decade, the scope, scale, and speed of Information Warfare (IW) will expand, radically transforming the future of conflict. IW attacks will sow disorder, mistrust, and radicalization to sway the sentiment of the public and the fighting force, at times compelling them to violence against institutions, organizations, and each other. The U.S. Army recognizes this trend in information-age warfare and seeks to address the phenomenon in its latest concept manual, The U.S. Army in Multi-Domain Operations 2028.[1]

This emerging information warfare attack plane stretches across three domains: digital, cognitive, and physical. Conflict will move swiftly, freely, and simultaneously between the three domains. Future attacks will utilize new technologies in novel ways and employ algorithm-on-algorithm conflict beyond the scope of human observation. These emerging factors will fundamentally change our understanding of conflict and require a new model to comprehend and operationalize the changing character of war. The information warfare framework (IWF) explained in this report is intended to assist military leaders and staff members with understanding, visualizing, describing, and directing operations on the 21st century battlefield.[2]

In the 20th century, the U.S. military viewed the state of conflict as a binary matter. We were either at war or peace. Conversely, in the 21st century, the global population's exponential adoption of powerful information technologies is causing cognitive effects that force military thinkers to approach conflict using a quantum perspective in which multiple states of conflict exist simultaneously from interactions across the digital, cognitive, and physical domains. To comprehend the future of conflict, it is necessary to move from a binary or Newtonian way of thinking and adopt Quantum state approaches where the nation can be both at war and at peace at the same time. The state of war or peace depends upon the observer, the circumstances, and context under which observations are made.

In the future, the definition of battlefields, combatants, and adversaries will need to be remapped in ways that contradict and challenge existing procedures and doctrine. In the era of great power competition, commanders on future battlefields will need to converge all capabilities, both traditional and emerging information-related capabilities in novel ways across the competition, conflict, and return to competition phases of multi-domain operations. This report provides examples of future threats intended to assist commanders in envisioning what conflict could plausibly look like in 2028. It is a strategic foresight tool intended to encourage further analysis and study of future information warfare threats. The report does not capture all possible threats, but it does present a number of plausible threats and actions the military can take to disrupt, mitigate, recover, and defeat future information attacks.

Future Information Warfare Threats:

- Alternative Facts become Alternative Realities
- Psychological Targeting
  - Emotional Hacking in Underlying Systems / Cultural Exploitation
  - Individual Psycho-Targeting for Military Gain
  - Psycho-Targeting of Country Cultures to Enable Disorganization
- Increased Divisiveness Creates Political Localism
- Domestic Strife Leads to International Vulnerabilities
- Breaking the Bio/Digital Divide

New Threat Actors:

- Information Oligarchs and Information Capitalism
- Elected Vigilantes

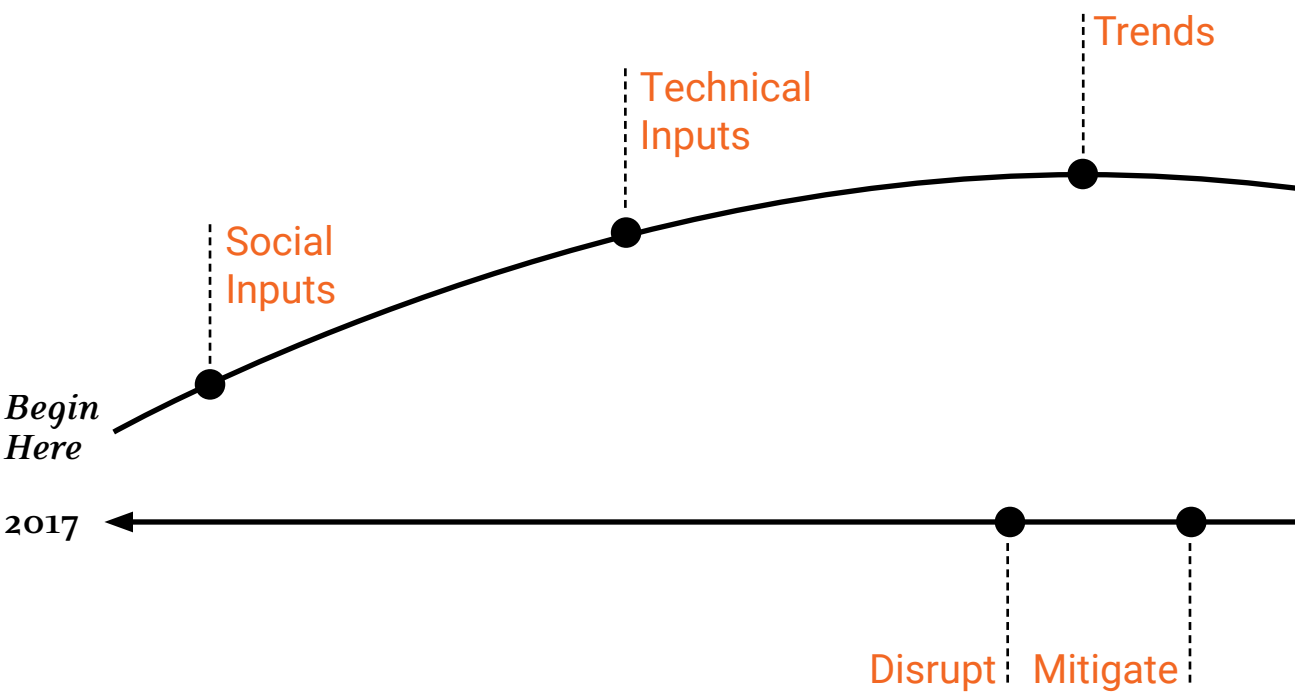
[1] Training, US Army, and Doctrine Command. "TRADOC Pamphlet 525-3-1 "The US Army in Multi-Domain Operations 2028,"." Training and Doctrine Command, Ft. Eustis, VA,(6 December 2018), viii–x (2018).

[2] Army, U. S. "FM 5-0 The Operations Process." (2010).

THREATCASTING
A BRIEF OVERVIEW

Threatcasting is a conceptual framework and process (Figure 1) that enables multidisciplinary groups to envision and plan systematically against threats ten years in the future. Groups explore how to transform the future they desire into reality while avoiding an undesired future.[3]

Threatcasting uses inputs from social science, technical research, cultural history, economics, trends, expert interviews, and even a little science fiction. These various inputs allow the creation of potential futures (focused on the fiction of a person in a place doing a thing). Some of these futures are desirable while others are to be avoided. By placing the threats into a fictional story, it allows decision makers and practitioners to imagine what needs to be done today as well as four and eight years into the future to



empower or disrupt the targeted future scenario. The framework also illustrates what flags, or warning events, could appear in society that indicate the progress toward the threat future.

Threatcasting is a human-centric process, and therefore the humans that participate in a threatcasting session are critical. Regardless of age, experience, or education, all participants are considered practitioners. Threatcasting is a theoretical exercise undertaken by practitioners with special domain knowledge of how to specifically disrupt, mitigate, and recover from theoretical threat futures. Additionally, a few participants are curated to be outliers, trained foresight professionals, and young participants for a fresh and multi-generational perspective in the groups. When using threatcasting on military problems, the mixture of participants should span academia, private industry, government, and the military.

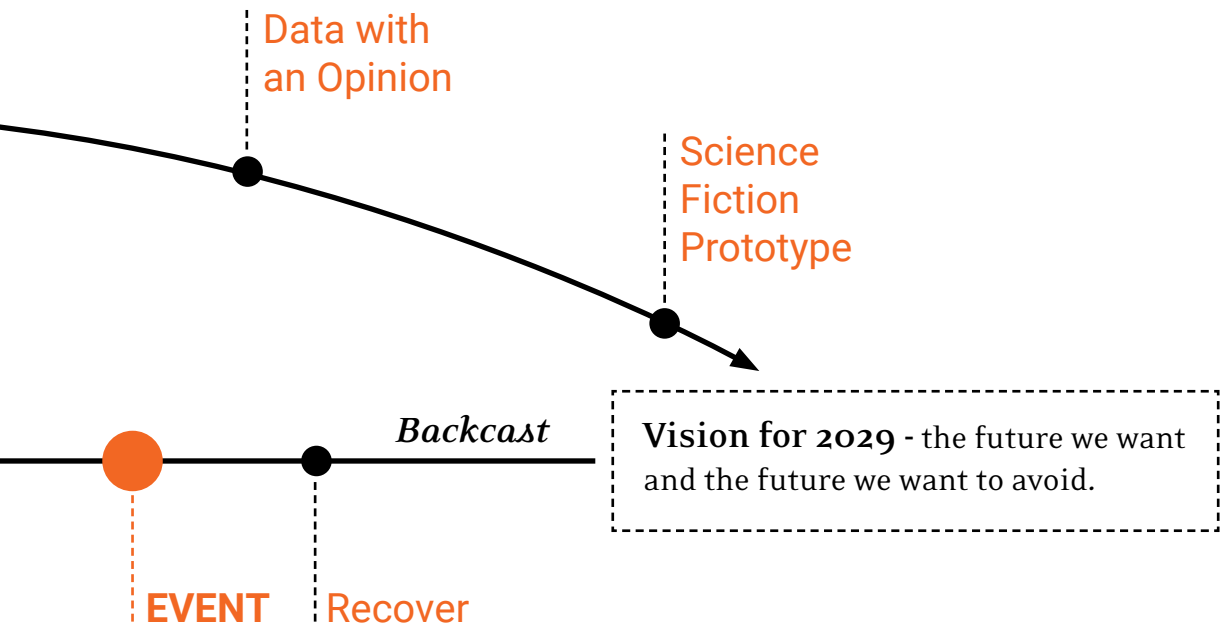


Figure 1

[3] Citation for Threatcasting paper

THE INFORMATION WARFARE THREATCASTING PROJECT

The goal of the Future of Information Warfare Threatcasting Project was to explore the coming decade's emerging technological and cultural trends and envision plausible future threats from multiple perspectives. The project sought to illuminate emerging areas of strategic threat and potential investment, particularly relating to the proliferation of emerging intelligences, technologies, and systems that could considerably change the nature of the battlefield by 2028 and beyond.

In three Threatcasting Workshops a select group of practitioners from across multiple domains (security, academia, media, and technology) worked to envision these futures and explore what actions should be taken now to counter future IW threats. The final goal was to operationalize the finding for the Army and to determine what actions could be taken to disrupt, mitigate, and recover from these future threats.

The initial Threatcasting Workshop focused broadly across the globe and society, exploring the implications of IW on citizens, governments, militaries, corporations, and other organizations. The main output from this session was the identification and definition of Information Disorder Machines (IDM) and their potential impacts on the future of the United States of America.

The second Threatcasting Workshop narrowed the scope to focus specifically on IW within the context of The U.S. Army in Multi-Domain Operations 2028 concept (TP 525-3-1). The threats and findings from this session identified a range of possible and potential threats, illustrating a shift in the character of conflict.

The third workshop collaborated with students and faculty at the Naval Postgraduate School in Monterey, CA during a Backcasting deep-dive on the two amalgamated future threat scenarios. This additional round of analysis specifically focused on outcomes from our previous two information warfare Threatcasting workshop and emphasized actions the Department of Defense (DoD) can target in the coming decade to disrupt, mitigate, recover, or defeat the cognitive and physical effects of information technology driven disinformation attacks during military operations.

COMPONENTS FOR THE FUTURE OF INFORMATION WARFARE

While there is currently no official U.S. government definition of Information Warfare, it is typically conceptualized as the use and management of information to pursue a competitive advantage, including offensive and defensive efforts.

> "Information Warfare: Issues for Congress"
> Updated March 5, 2018
> Congressional Research Service
> R45142

The rise of the "Information Age" has seen greater connectivity, rapid access to personalized content and information, and a greater network effect across our social, professional, and academic lives. This increased connectivity also enables serious vulnerabilities. Along with the benefits of the information age, we should also recognize that actors, both benevolent and nefarious, can leverage increased access to information for strategic advantage. For the Army, this means that information exchange as well as network understanding and monitoring will become increasingly important, if not the biggest factors in warfare strategy in the coming decade. This shift in battlefield from kinetic effects toward networked and information-driven effects is beginning to be explored by multiple arms of the military.

"The final development of Third Wave war may well be the conscious design of something the world has not yet seen: competitive knowledge strategies."

Alvin and Heidi Toffler
Futurists and bestselling authors of Future Shock

The 2012 Air & Space Power Journal described this shift in battlefield thinking by outlining that "in today's network-centric battlespace, the victor must not simply attack and exploit the enemy's cyber and communication systems at the tactical level but completely understand the information environment."[4] Deep understanding of the multi-faceted information environment is paramount to creating a strategic advantage for any military operation in the decade to come.

Recently the RAND corporation investigated the future of IW, publishing a report titled Strategic Information Warfare: A New Face of War - bringing together a number of perspectives on the evolving nature of Information Warfare and its particular impact on U.S. defensive strategies. The report argued:

> **"Future U.S. national security strategy is likely to be profoundly affected by the ongoing rapid evolution of cyberspace--the global information infrastructure--and in this context by the growing dependence of the U.S. military and other national institutions and infrastructures on potentially vulnerable elements of the U.S. national information infrastructure".[5]**

Both the RAND report and Threatcasting highlight and emphasize that the IW battlefield is rapidly evolving with the invention, restructure, and deployment of increasingly advanced technology. The expansion and integration of emerging technologies by military, industrial, government, and civilian systems such as Artificial Intelligence (AI), Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), smart cities and environments as well as Internet of Things (IoT) devices, will significantly impact the size of the IW attack plane. More importantly the interplay between these technologies will amplify the impact of attacks. As technologies become increasingly more interoperable, the opportunity for large scale systematized attacks grows. Given the growth of technological interoperability, the exact outcomes can be highly mutable. Through this report, we have identified several threat vectors that will assist in making potential threats more tangible.

[4] Mark Ashley, "KWAR: Cyber and Epistemological Warfare—Winning the Knowledge War by Rethinking Command and Control," Air and Space Power Journal 26, no.4 (July–August 2012): 58, http://www.airpower.au.af.mil/digital/pdf/issues/2012/ASPJ-Jul-Aug-2012.pdf.

[5] Strategic Information Warfare: A New Face of War. (n.d.). Retrieved from https://www.rand.org/pubs/monograph_reports/MR661/index2.html.

Reflexive Control

Reflexive control originated as a Soviet idea in which one “conveys to an opponent specifically prepared information to incline him/her to voluntarily make the predetermined decision desired by the initiator of the action”.[6]

In context of IW, reflexive control is a tactic which includes a sustained effort at shifting the behavior of specific targets by ingestion of specific data, where the ultimate goal is to get that target to achieve an action that is to their advantage - ideally without the target becoming aware of their manipulation. This method of attack plays fundamentally on the underlying cultural understanding, psychology, or dogma of the intended target - exploiting existing biases or creating new ones in order to manipulate behavior and actions.

Information Disorder Machines (IDMs)

The emerging threat of IDMs lie in the unique pairing of their real-time microtargeting capabilities and the scalability of their macro effects.[7] In the coming decade, advances in technologies like artificial intelligence (AI), machine learning (ML), quantum computing, the internet of things (IoT), smart cities, and autonomous vehicles in land, sea and air will enable adversaries of the United States to mechanize information disorder to influence, manipulate, and harm organizations or individuals at scale. IDMs will be targeted broadly at groups and geographies. AI and ML will allow for increased, if not complete automation, allowing IDMs to adapt in real-time down to the individual level, creating personalized attacks while operating at a mass scale. This is a direct threat to national and global security. The potential of IDMs poses a significant danger to the future of democracy in the United States of America.

IDMs specifically target the underlying social and cultural beliefs held by individuals, groups, and geographies. Leveraging knowledge unique to specific target groups, IDMs can manipulate, direct, or mask behaviors based on the ability to disseminate information in real-time across large populations. As humanity's reliance on direct access to information and content increases, so do the vulnerabilities for the precise targeting and manipulation of that information.

[6] Kowalewski, Annie. "Disinformation and Reflexive Control: The New Cold War." Georgetown Security Studies Review, July 22, 2019. https://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/.

[7] Johnson, Brian David. "Information Disorder Machines: Weaponizing Narrative and the Future of the United States of America." Technical Report. 2019. Tempe, AZ: Arizona State University. https://threatcasting.com/publications/

THREAT FUTURES

INVISIBLE FORCE

A SCIENCE FICTION PROTOTYPE

UN Mission to North Africa 2030

They are destroying our holy sites…

Mamane stared at his phone with horror and disgust. Under the tag #NoJustice there were videos, testimonials and postings from local civilians on the northeast border. The UN forces occupying the region had targeted sacred sites...

The footage showed UN troops, mostly Americans, destroying holy sites, while prisoners sat on the floor, their hands zip tied behind their backs. The women screamed. The troops laughed…

Mamane grabbed his friend. "Look, look what they're doing now…"

Theodor glanced at his friend's screen for a moment and then looked away. "I can't watch," his voice was tight with rage. "I can't watch. Did you see that their aid workers are vaccinating children with cancer? "

It showed him the conflict behind the conflict. The unseen battle between their code and our code.

"We have to do something about it..." Mamane locked eyes with his friend.

"I know," Theodor replied coldly.

The mob outside the base continued to

grow. Intelligence Officer MAJ Diego Garcia could tell the size by the volume of the chants and the amount of gunfire. They were shooting in the air...for now...to show their rage.

The brigade wasn't expecting the mob to grow so large, but it didn't surprise Diego. He leaned in, watching the updates stream across the screen.

"See this," he tapped a posting.

"What's that?" Adele, his French counterpart with the UN mission, replied.

"See this whole string?" Diego continued. "None of it's real...the deep fake content shows us raping women up here on the border."

"The quality has gotten better," Adele replied. "Even since last week...How did it get out?"

"That's what I'm trying to figure out...."

Diego pushed aside the postings and pulled up INVISIBLE FORCE. It showed him the conflict behind the conflict. The unseen battle between their code and our code. Even if it was hard for Diego to discern who they were...

"It looks like someone got directly into the network," he said after some searching. "This whole thing is a mess," he grunted.

Adele's phone buzzed in her pocket. Pulling it out she checked to see if it was her mother in Paris posting about her father's surgery...

Diego didn't take notice.

"MAJ Garcia, sir," CPT Schultz rushed into the room. "The locals...the mob sir...we have a problem..."

It was then that Diego heard the change in the gunfire...they were no longer shooting into the air...

Before they could move, the inbound rocket struck the room killing all three soldiers and wounding two others nearby.

THE BILL LUMLEY SHOW

Fairfax, MD

"Good evening everyone and welcome to the Bill Lumley Show, I'm your host and chief agitator Bill Lumley..." the podcast began. About fifty thousand listened live to Bill, but more than a million listened in the week following.

"So, tonight's topic is...Why are we still involved with the UN? I mean have you seen these reports coming out of the northeast border settlement. They don't want us there... we don't want to be there...I mean come on people how many more of our service men and women need to die? I wanna hear what you think...call me, post, go directly to our podcast...let's fix this thing..."

(Red Pawn 3)

INFORMATION WARFARE THREATS

Information Warfare (IW) is a concept involving battlespace use, management, and the maneuver of information and related technologies to gain competitive advantage over an adversary. The following threats engage predominantly within the social / cognitive area of the IW framework. While unique, each threat vector carries certain nuances that will illuminate distinct differences in either the preparation for, engagement with, or understanding of potential emerging threats. These vectors will utilize advancements in technological platforms, including artificial intelligence (AI), machine learning (ML), virtual reality (VR), augmented reality (AR), mixed reality (MR), the Internet of Things (IoT), and smart cities technologies.

The threats identified in the IW Threatcasting Project demonstrate how IDMs will be engaged within a broad attack network - both foreign and domestic. The novel aspect of these social / cognitive IW threat vectors is their focus on leveraging, disrupting, or manipulating underlying belief mechanisms that reside within citizens and military personnel alike, in ways that digitally manipulate physical behaviors. No longer will attack strategies solely target an identified digital or physical target but will target the underlying psychology of the target's operator first - allowing a much more pervasive and culturally destructive attack to take place long after initial contact

THREAT:

ALTERNATIVE FACTS BECOME ALTERNATIVE REALITIES

Several threat futures identified situations where immersive content becomes the only content for individuals, yielding ever more real worlds that are based on virtual curation and manipulation of existing biases. Manipulation focused on subtly introducing and reinforcing ideas that challenge election security, confidence in democratic institutions, and vulnerabilities inherent in social media platforms – particularly through the viability and wildly unchecked use of fake news.

In these situations, subjects confuse the online world of extreme echo-chambers for the real world, being reflexively controlled based on confirmation of their radical. IDM's adjust and elevate the targeted individual's biases by exploiting the gap between the pervasive deep fake content they consume and societies technical abilities to disprove the truthfulness of the deep fake .[8]

THREAT:

PSYCHOLOGICAL TARGETING

1. Emotional Hacking of Underlying Systems / Cultural Exploitation

Future attacks will target cultural undercurrents as vulnerabilities; exploited particularly through subconscious introduction of new mantras in gamified digital environments to sway participants toward mal-intended outcomes. This cultural exploitation also takes the form of manipulating belief systems through propaganda-like sub- or inter-conscious messaging via immersive streaming platforms.

Several threat futures focused on deliberate and longitudinal manipulation of education systems as an active measure within the auspices of information warfare that move beyond traditional propaganda.[9] These temporal attack vectors implement strategies that subtly work to revise recorded events to shift the targeted public's thoughts and beliefs in a manner that support the goals and objectives of the attackers. Active and continuous information manicuring effectively alters or erases aspects of digital history as a form of damnatio memoriae[10].

[8] Raw Data Examples in Appendix: extreme information divide specifically to take down democratic process (purple pawn 2, black pawn 2), seeding discontent to open up business lanes (red pawn 3).

[9] Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." Connections 15.1 (2016): 5-31.

[10] Raw Data Examples in the Appendix : sub- or inter-conscious propaganda (orange pawn 3, teal pawn 2, teal pawn 3, red pawn 1)

THREAT FUTURES

ACROSS A DARK CHASM

A SCIENCE FICTION PROTOTYPE

Training Area in Eastern Europe - 2030

"They just don't care anymore..." SFC Joe Gilbert sighed, leaning back in his chair, tilting his head up to the ceiling. He was tired and his eyes hurt from reviewing the day's training data.

"Did you see what they did last night...when they thought we weren't paying attention?" SFC Phil King replied. He too had his head tilted to the ceiling. "It was your boy Antoni. They say he was the one who started it…"

"No what?" Joe clicked off the full VR from his glasses so he could see Phil. "I didn't see anything…"

"You didn't see it?" Phil clicked off the VR and shook his head. "Antoni was down at the bar last night saying how everyone in his country wanted us to leave and if we didn't leave then it would be up to him and the rest of them in the bar to kick us out...I can't believe we are wasting our time in this place…"

"It doesn't surprise me," Joe replied. "I barely see Antoni anymore…"

"Well we're going down there tonight…" There was an angry pause in Phil's voice. "I wanna see what they say when we're there…"

It was past midnight and Joe walked quietly down the hall of the empty training center. He was tired but couldn't sleep again...it had been weeks since he had a good night's sleep. He didn't want to talk to anyone, so he'd taken to pacing in the center until he passed out.

What were tonight's troubles? Joe couldn't understand why Antoni would say that. They had been training partners when Joe arrived three months ago for the emergency deployment training. They were friends once…

Joe turned the corner and froze. There was another person in the center.

"I know you are sleeping with my sister," a familiar voice said.

"What?" Joe replied, turning on the light. "Is that you Antoni? What are you talking about…"?

"I know you are sleeping with my sister…I've seen your posts…I've seen what your buddies have been saying about us…" Antoni repeated, his hand shook as it hovered over his side arm. His eyes were tired and bloodshot.

The sight of the gun put Joe on alert. "Is this a joke? What are you talking about? I don't even know your sister...I'm married...you know that...my wife is back at Fort Bliss… What posts?" He tried to get a reaction out of Antoni, but he looked dazed. "Is this a joke? Is this about what you said at the bar last night?"

"I don't drink," Antoni replied flatly. "You know that…"

Both soldiers stared at each other tensely across a wide dark chasm. Each stood in his own reality. The distance between them was electric and dangerous.

The two men heard sirens in the distance. They didn't yet know that a fight had broken out at the bar. Nor did they know who had been subtly, daily widening the dangerous chasm that separated them.

Both soldiers stared at each other tensely across a wide dark chasm. Each stood in his own reality. The distance between them was electric and dangerous.

THREAT:

PSYCHOLOGICAL TARGETING

2. Individual Psycho-Targeting for Military Gain

Through deep psychological profiling of cultural upbringing, belief systems, and the educational paradigms of specifically identified targets, bad actors manipulate actions of the targeted within a military construct. Discrete actions by individuals add up to a pervasive undermining of trust in digital military network and battlespace visualization tools. Adversarial knowledge about the psychological operations of their targets enable them to hack into the subconscious, turning loyal military personnel into unknowing inside-actors through simple data point manipulations.[11]

3. Psycho-Targeting of Country Cultures to Enable Disorganization

The psychoanalysis of a country leads to exploitative opportunities based on the prevailing dogma within that nation's cultural system. An individual's priorities will often lie with cultural belief systems that have been built into a culture over generations. For example, in Japan it may be the importance of preserving family honor. In the US it may mean preserving our interests in acting as protectors for our valued allies. Targeted attacks that exploit psycho-cultural vulnerabilities are effective at getting the targeted society to behave in ways that benefit the attackers (reflexive control) - particularly as a distraction while simultaneously conducting attacks on larger networks.[12]

THREAT:

INCREASED DIVISIVENESS CREATES POLITICAL LOCALISM

Several threat vectors identified themes that involved instigating emotionally charged domestic debates and fomenting political strife as active measures. Threat vectors predict that states and local governments will become increasingly insular, opening up opportunities for adversaries to launch attacks that undermine social trust in political leadership at local, state and federal levels. Attacks of this nature will be purposefully limited to smaller geographical areas to avoid early detection. Information attacks designed to divide were found to be initiated in multiple geographically bounded areas while simultaneously rippling across all levels of government with the goal of destabilizing crumbling democratic systems from the bottom up.[13] Current examples of this phenomenon are the current successionist movements found in California and Texas. Adversaries will deploy IDMs that exploit the fissures between parties on both sides of this issue in the future.

[11] Raw Data Examples in Appendix: sinking a japanese ship she thought was russian (black pawn 3), sinking a friendly ship she thought was hostile (yellow pawn 3), non-military podcast propaganda (orange pawn 1)

[12] Raw Data Examples in Appendix: US savior complex (purple pawn 3), japanese familial honor (yellow pawn 1)

[13] Raw Data Examples in Appendix: military mistakes leads to national government distrust (yellow pawn 3), information siloing leads to secession talks (orange pawn 2)

THREAT FUTURES

CONSENT OF THE GOVERNED

A SCIENCE FICTION PROTOTYPE

Denver, CO - September 4, 2030

Denver Police Chief Olivia Marsh waited in the governor's office. She was not a patient woman, but she didn't have a choice. Governor Len Barker was late. Len was always late.

The media and a crowd had already started to gather on the front steps on the steps of the Colorado State Capitol building. Just to be safe Chief Marsh shut down Grant, Lincoln and 14th Ave. She wasn't expecting trouble but these days…

"The Antifa faction in Portland, Oregon has occupied all of downtown from the Willamette River up to NW 23rd ave," Ashwini continued her report. he young woman was an aid to Governor Barker, specifically tasked to monitor the protests and violence around the presidential election. "Arizona, New Mexico and Texas have all committed to move forward with their local secession votes even after the Supreme Court ruling.."

"That was expected…" Chief Marsh replied. This briefing wasn't scheduled but the Governors staff was trying to keep her busy while Len made his way through traffic.

"Yes ma'am," Ahswini nodded nervously.

"The race riots in Richmond have disbursed but the White Power faction has said they are going to Atlanta. The President is calling on the internet carriers to cut off service…"

The United States was pulling itself apart little by little, protest by protest, riot by riot. What had been simmering on the internet for years with only small flash points had become widespread and violent at the start of the election year…

"Governor Barker is pulling up," another staffer stuck his head in the office. "He says he'll meet you by front security."

Chief Marsh rose from her chair. With a sigh she breathed, "Let's get this party started…"

Chief Marsh approached the microphone. Governor Barker stood behind her a little to the left. She scanned the steps of the Capitol Building packed with media and interested onlookers.

"All of you who know me," she began. "And those of you who don't will learn real quick that I don't beat around the bush. I'm going to say a few words and then Governor Barker here will say some remarks. I will not take questions…" she paused, glancing over her shoulder. "I'll leave it to the Governor to decide if he will take questions."

While Chief Marsh spoke camera flashes flickered incessantly. All cameras and microphones were pointed squarely at her face.

"Ok..." she continued. "I am officially announcing today that the city of Denver and indeed the state of Colorado will hold local and national elections as scheduled. We are aware that the President of the United States has moved to delay federal elections in light of recent unrest and violence... However, the state of Colorado believes that democracy needs to be done."

"You don't have the authority," a voice yelled from the audience.

"Has the President made good on sending in the Reserves to delay the elections?" another asked from the reporters.

Chief Marsh paused then continued. "I will not be answering questions at this time. Suffice it to say Colorado believes in democracy and we will call on other states to uphold the Constitution...Now I will turn over the mic to Governor Barker…"

(Black Pawn 2)

The United States was pulling itself apart little by little, protest by protest, riot by riot.

THREAT:

DOMESTIC STRIFE LEADS TO INTERNATIONAL VULNERABILITIES

Informational threat actors will continue to exploit the rise of populism within democratic societies based on trends in mass immigration, climate change, ideological differences, and political polarization. The U.S.'s adversaries will continue to reinforce this phenomenon, both domestically and internationally. The purpose of these information tactics are reflexive control mechanisms designed to sow chaos and create division among diverse populations in democratic nations. The confusion created from these events are intended to defeat any measure of efficient and popular consensus between the multiple parties that normally control power within democratic societies. Threat actors will exploit the high degree of free speech and loosely regulated use of social media platforms found in western democracies. The effects of these attacks will continue to reinforce political polarization between trusted media sources both locally and domestically.

Increased populism within the U.S. will continue to polarize the political process - causing delayed understanding and decision making in both domestic and international affairs. Nation-state threat actors will capitalize on the U.S.'s crippled sense of understanding and decision to achieve their strategic goals and objectives while experiencing little military or diplomatic resistance from America or her allies. Adversaries will continue to propagate disinformation across America's political, cultural, and ideological echo-chambers. This polarizing strategy is a distraction mechanism that feeds disinformation intended to fuel anger, fear, and chaos throughout the U.S.'s diverse population. Threat vector narratives found in this research illustrate techniques in which adversaries use subtle and nuanced disinformation techniques that simultaneously stir the emotions of diverse groups at the local level within the U.S. These attacks are varied, powerful, and often disconnected from national media sources. Localized disinformation attacks using advanced technologies, such as deep-fake content, will cause cultural, social, economic, political, and geographic fissures across the U.S. that adversaries will continue to reinforce and exploit. If these attacks continue to remain unchecked, U.S. sovereignty over its boundaries, populations, and regional control could be assumed by adversarial threat groups.[14]

[14] Raw Data Examples from Appendix: biological Typhoid Mary via social media streams (red pawn 2)

THREAT:

BREAKING THE BIO/ DIGITAL DIVIDE

In a future where physical and digital worlds are converging using advanced technologies; the biological world is not immune. The separation between biological and digital worlds will crumble through the adoption of technologies, such as bio-chipping and augmented reality, significantly increasing the intersection between these worlds as an attack plane. As global populations adopt bio-chipping to enhance performance, manage vulnerable organs, and monitor human activities it will present new vulnerabilities. Threat actors will use similarities between digital and biological codes, particularly in bio-chipping devices, as new dissemination networks for perpetrating viral attacks using biomimicry. The U.S. military's adoption of these technologies will be extensive and present the same inherent technical vulnerabilities found in the commercial-off-the-shelf (COTS) devices used by non-military populations. The expanded digitization and networking of the biological world through human implanted network devices, greatly increases the information attack plane creating the potential for powerful new and viral bio-digitized attacks that create a whole new attack dimension on future battlefields.

[15]Raw Data Examples from Appendix: biological Typhoid Mary via social media streams (red pawn 2)

THREAT FUTURES

PATIENT 00110000

A SCIENCE FICTION PROTOTYPE

Charlotte Douglas International Airport, Charlotte, NC - 2030

"I don't know why they always put us in that hotel…" Birdie Sittenfeld tried not to yawn but couldn't help it.

"I think they did a deal like a year ago," Shelia replied flatly. The two flight attendants had slept poorly and had to get up early for the flight to New York they were working together.

"I didn't get but a few hours," Birdie yawned again.

When they reached the gate, it was still empty.

"You want a tea?" Shelia asked.

"That would be lovely dear," Birdie nodded. "Two sugars please."

Sheila left her bags behind and walked deeper into the terminal. Birdie looked up at the TV screen just as it switched to breaking news.

"We have breaking news from Helena Montana and the site of the Montana State Capital Occupation…"

Images of the embattled building flashed on the screen...smoke rose from the dome…

"Extremist activists who have been occupying the state capital for the last ten days have cut off communication with police, calling them a part of the conspiracy. That in fact the police were behind the BioChip Plague... Local law enforcement and

"Extremist activists who have been occupying the state capital for the last ten days have cut off communication with police, calling them a part of the conspiracy.

the national guard are preparing to enter the building... "

Armored vehicles moved across the front lawn. Spotlights slashed through the early morning darkness…

"Those poor people," Birdie said out loud and touched her chip. It had always had a funny little scar around it...ever since she was a little girl.

"This is yet another violent turn in this evolving story around the mysterious BioChip Plague... as many have been calling it," the report continued. "Protests have broken out in Seattle, St. Louis and Atlanta. In many cities in the north east, parents are keeping their children home from school...the unrest has worsened at the southern border as major infrastructure failures have…"

Something was happening in the terminal. The early morning quiet started to rustle with movement. Birdie could see movement near the coffee shop where Sheila had disappeared.

"Attention...attention…" The PA system began. "For your safety, please shelter in place...Attention...Attention…"

Figures in bright orange hazmat suits ran towards Birdie. They were followed by emergency carts and ATVs with large rolls of plastic.

"Birdie Sittenfeld!" one figure with a megaphone bellowed. "Birdie Sittenfeld! Do not move! I repeat, do not move!"

Birdie was frozen in fear. Teams were clearing out all the other terrified people in the terminal.

"Are you Birdie Sittenfeld?" one asked through his protective visor. He was out of breath and the mask was fogged up.

"Yeh...yes." Her knees began to shake.

"I have her!" the man yelled into his headset. "I have her! Patient Zero is in Terminal B... Gate 85...we are clearing and securing the area…"

"What's wrong," Birdie shook all over as the team surrounded her. Some began to unroll large sheets of plastic.

"I told you that plastic is not going to help," someone yelled. "It's digital…"

"Ms. Sittenfeld," a woman, also in a hazmat suit approached. "Were you in Athens Greece on the 12th of August this year?"

"We know that," the man blurted out. "You don't need to…We checked her route! They all match up..."

"I need to verify…" the woman snapped back. "We don't even know what this BioChip Plague thing is…"

Birdie got dizzy. She remembered the trip to Athens with friends...it had been wonderful... but all those cities…

She remembered the reporter's voice... Seattle. St. Louis. The southern border… San Diego. San Antonio. Those were all a part of her route...Patient Zero...that terrible plague…

Birdie lost consciousness.

"I told you that plastic won't help!" someone yelled again.

(Red Pawn 2)

NEW THREAT ACTORS

The world's evolving technical landscape creates the continuous emergence of new threat actors. While state-sponsored and independent terror actors will continue to populate the landscape, new bad actors of all different types will emerge due to the expansive adoption of network technology installed in nearly every device and increases in the world's technically educated population. Not only will data and information become new bargaining chips, but the systems that enable access and set precedent around cultural norms for data usage will become part of the playing field. New tactics will emerge for the use and misuse of these systems, dissolving rules around who can use what tactics, and blurring the lines between criminal actions and lawful usage.

THREAT ACTOR:

INFORMATION OLIGARCHS AND INFORMATION CAPITALISM

With the generation of increasing amounts of data and supportive platforms, businesses will capitalize on the emerging information trade market. Owned information creates an information access divide, particularly surrounding the urban / rural technology split. Those leaders that created early dominance are now realizing the power inherent in data stewardship. Information, content, infrastructure, and access will all be manipulated, controlled, and distributed putting capitalist values ahead of public access rights. The power of control over data and information access will be corrupted, exploited, or otherwise turned toward causing harm with impacts at a larger scale. [16]

THREAT ACTOR:

ELECTED VIGILANTES

Taking cues from hacktivist campaigns, governments will enter a new era of social and political manipulation. As boundaries both digital and physical continue to blur, the boundaries between government and criminal actors similarly blurs. Governments and public organizations will turn toward tactics traditionally used by criminal organizations for the express purpose of maintaining public safety. Using these means, however, will open up these systems for misuse, attack, or exploitation for nefarious means.[17]

[16] Raw Data Example from the Appendix: information capitalism - textbook content manipulation (teal pawn 1) info oligarchs and urbanized access priority (purple pawn 1), control of non-critical infrastructure toward large scale behavior manipulation (black pawn 1)

[17] Raw Data Example from the Appendix: govs taking cues from criminal actors (yellow pawn 2), and govs acting like criminal actors (purple pawn 3)

THE INFORMATION WARFARE FRAMEWORK (IWF): A MODEL FOR THE FUTURE OF CONFLICT

The threat landscape explored by the IW Threatcasting Project uses a functional model to describe and explain the future of conflict and the changing character of war in the 21st Century.

The Information Warfare Framework (IWF) illustrates the components of Information Warfare, categorizing them into distinct domains of conflict; the physical, information, and social / cognitive domains. These domains and their intersections with one another create a holistic picture of plausible conflict trajectories for IW. (Figure 2.) Each domain is important to consider individually, but it is at the intersection of all areas where we will find the most integrated understanding of IW and its potential impacts.

This kind of framework has been used in the past to explain the workings of Cyberspace for an organization or firm.

"Cyberspace consists of three interdependent physical, informational, and cognitive dimensions. These dimensions continuously interact between systems, individuals, and organizations both within and beyond the firm.

Physical Dimension: Devices, wired and wireless networks, and sensors of both information technology and operational technology

Informational Dimension: Data, information, knowledge, and software (semiotic perspectives of human perception)

Cognitive Dimension: The human mind; employees, customers, rivals, and stakeholders (sensemaking and meaning making)

"Technology is a strategic asset not only for the firm, but also for hackers who understand how to leverage a firm's own technology investments to facilitate theft, hijacking, and manipulation of a firm's data, knowledge, and core capabilities for profit. A lack of an adaptive cyber capability puts a firm at risk but building a dynamic adaptive cyber capability can lead to significant reward outcomes, and can facilitate the growth of new capabilities and resources."[18]

Increasing technological complexity and a widening informational attack plane reveals that this expanded functional model is needed to understand conflict in the 21st century. We are not asserting that the nature of war is changing but that the methods in which war is being waged are changing and in profound ways. Increasingly powerful, cheap, and easily accessible information technologies are being leveraged and will continue to be leveraged in novel ways on the 21st century battlefield. These changes require an expanded mental model for understanding shifts in the ways and means in which current and future conflicts are being prosecuted.

[18] Schwartz, T. Schuff D. "The Cyber-Based View of the Firm - A FRAMEWORK FOR SURVIVAL IN THE INFORMATION ECONOMY". The IBIT Report - A Publication of the Institute for Business and Information Technology. 2018

FROM BINARY TO QUANTUM

In the 20th century, the U.S. military viewed warfare using an analogy introduced by Clausewitz in On War, in which he compares warfare to "a pair of wrestlers" that through the use of "physical force each tries to compel the other to his will."[19] Military understanding of conflict resided on the continuum between war at various different levels of physical conflict or in a state of peace in which there was no physical conflict. Overall, 20th century warfare was viewed as a binary in which the military was either at war or peace. However, in the 21st century, we see rapidly increasing information technologies, the expanding impact of these technologies, and the cognitive effects these technologies have on societies as ushering in a new state of conflict.

The U.S. military can no longer afford to view conflict as a binary state. As demonstrated in early 21st century wars, conflict must now be viewed using a quantum state perspective. Conflict is no longer an either/or decision, our research establishes that conflict in the 21st century resides in two states simultaneously in which nations' can be both at war and at peace. Information Systems can be both secure and hacked at the same time depending upon who is investigating the system. Consumers of information can also believe or disbelieve the information they are consuming based on their bias-driven perspectives, regardless of facts, and dependent upon whether the conveyed narrative supports their beliefs. Therefore, truth, untruth, and belief in neither, all reside simultaneously within the minds of people.

To comprehend the future of conflict it is necessary to move from a binary or Newtonian state perspective to a Quantum state perspective in which a state of war and peace exists simultaneously. The state of war or peace depends upon the observer, the circumstances, and context under which the observers perceive information. In the future, the definition of battlefields, combatants, and adversaries will need to be remapped in ways that contradict and challenge existing strategies, procedures, and doctrine.

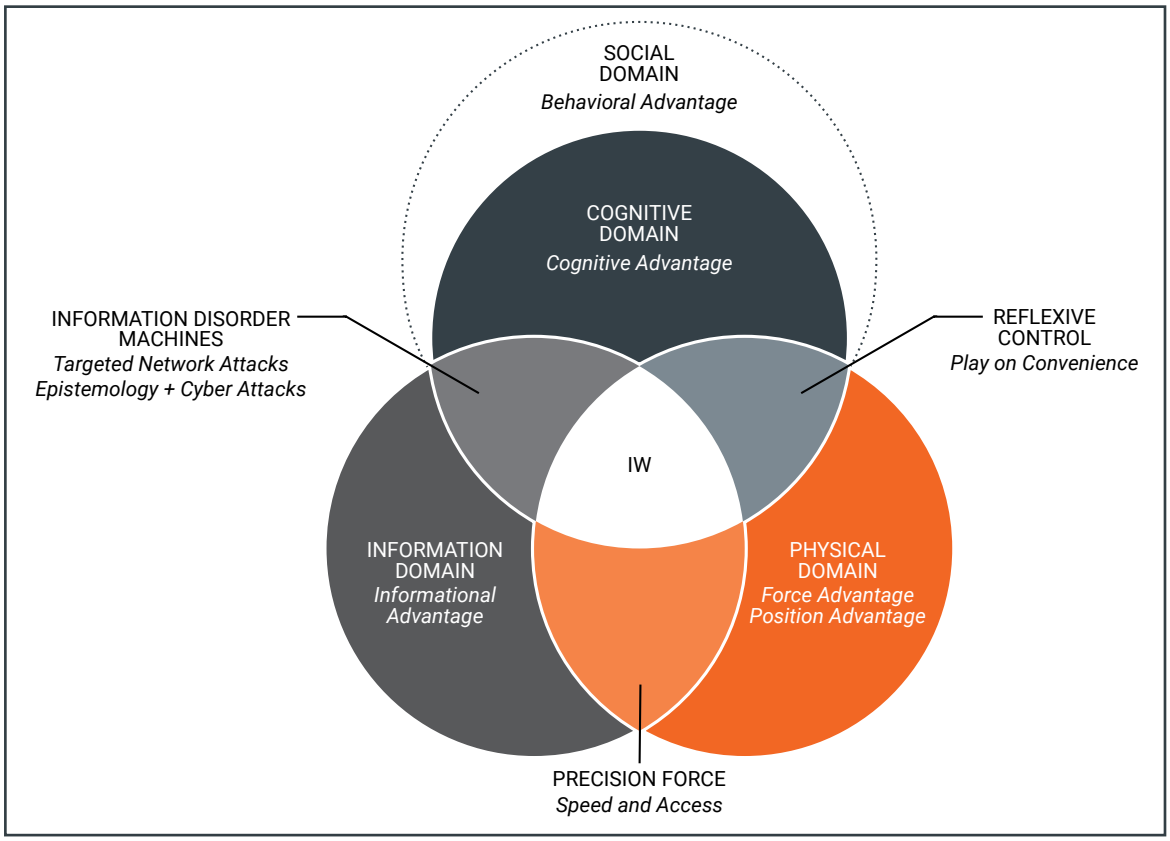


Figure 2 [20]

While each domain of the IWF contains potential threats to investigate for the future, the more complicated and dangerous may be the social / cognitive domain as it relies necessarily on the human target. Concerted focus in this report has been given to outlining key threats that engage specifically within the social / cognitive realm of IW in order to illuminate potential future threats. These threats will have additional implications for the information and physical domains and should be used as an initial investigation for further exploration.

Much of this report will focus on the social / cultural aspect of the IWF as most of the Threatcasting Work session scenarios, threats, and takeaways highlight this aspect of IW. The focus of this report, however, does not preclude or discourage directed investigation into other realms of the IWF. Investigation into the full IWF should be rigorously undertaken in order to best understand the future IW landscape.

[19] Von Clausewitz, Carl. On war. Vol. 2. Jazzybee Verlag, 1956. P. 75

[20] Adapted from Dr. Paul W. Phister Jr. and Mr. Igor G. Plonisch, Information and Knowledge Centric Warfare: The Next Steps in the Evolution of Warfare [Rome, NY: Air Force Research Laboratory, Information Directorate, n.d.], 7, http://www.dodccrp.org/events/2004_CCRTS/CD/papers/188.pdf.

INFORMATION WARFARE OPERATIONALIZATION

The third IW Threatcasting workshop concentrated on actions the Department of Defense could focus on in the coming decade to avoid, mitigate, or recover from the threats outlined above. The threats generated in the first two IW Threatcasting workshops served as an input to the backcasting exercise.

Five potential areas for action and operationalization emerged from this workshop.

1. UNDERSTAND THE DECAY OF THE AMERICAN "BRAND"

brand-image *n. the impression of a product in the minds of potential users or consumers; also transferred and figurative, the general or popular conception of some person or thing.*

In 2030, the American "brand" will have decayed and have far less resonance than it has had in the post-World War II eras. American ideals will not be as desirable. Alternative "brands" and ideals will become more favored to countries not yet at Western levels of development. China will become a popular technology trade partner within Africa. The dominance of Chinese-made information technology in exchange for economic incentives and natural resource rights is a partnership that does not rely on democracy, capitalism, or other American values.

- Despite efforts by military units at all echelons to partner with allied and future allied nations in military activities, there is a dearth of reinforcing activities from the diplomatic, economic, and national information programs that need to be leveraged to market America's "brand" in the 2030s.
- There are an insufficient number of foreign service officers and a lack of centralized national information programs and strategies available to provide alternative perspectives about American ideals.
- The military will carry a significant part of the load as the "face" of America. However, soldiers are not trained for this role. Generally the responsibility would fall to the Department of State.
- Possible areas for exploration: Review and assessment of the role of "The American Brand", specialized training, expanded recruiting, automated systems to augment human capital shortfalls, and face-to-face validation of relationships

[21] Oxford English Dictionary.

2. CONTROL OF THE NARRATIVE

Narrative *n. a representation of a history, biography, process, etc., in which a sequence of events has been constructed into a story in accordance with a particular ideology*

grand narrative *n. a story or representation used to give an explanatory or justificatory account of a society, period, etc.*[22]

The ability to "insert an American narrative into any system, at any time," a goal offered by one of the Backcasting teams, is a wide exclamation of hubris, yet is relatively common in military strategies.

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

A major strategic hurdle the U.S. must overcome to be informationally successful during multi-domain operations (MDO) is mastering the languages and cultures of our major global competitors (China, Russia, Korea, and Iran). The global impact of American movies, television, music, ideals, and culture have given these adversaries a considerable advantage in their understanding of the U.S. information landscape. The U.S. current lack of understanding and talent puts it at a considerable disadvantage.

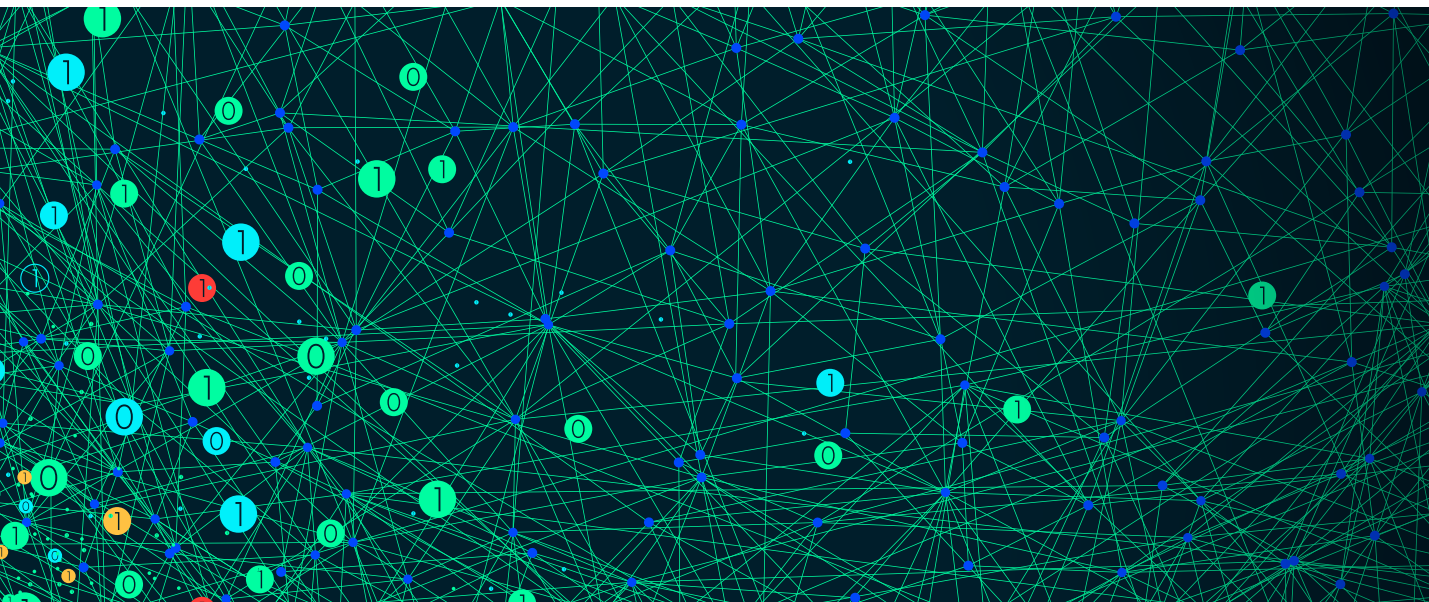
In the future DoD strategists will need to consider "culture" and "society" not as singular items, but as complex and nuanced systems that do not lend themselves to annual combatant command reports. Constant and persistent evaluation of military actions in relation to current events, cultural artifacts, and the subtleties between groups arranged by race, ethnicity, religion, geography, and socio-economic status are not factors that can be lumped into a single term.

"Narrative insertion" will require our intelligence and cyber operations to be fully connected into every system. Both Russia and China have strategies to balkanize and isolate their information flows in order to stymie both technical and informational connections.

- In late 2019, Russia demonstrated a proof of concept to isolate their national internet from the world.[23]
- In early 2020, China declared that textbooks not published in China were banned from its primary and junior high schools. Continued technical and cultural firewalling will further challenge the DoD's ability to insert our narrative anywhere, at any time.

[22] Oxford English Dictionary

[23] Chowdhury, H. (2019, Dec 24). Russia's test-run for its alternative internet a success, says Kremlin. The Telegraph. Retrieved from https://www.telegraph.co.uk/technology/2019/12/24/russia-successfully-tests-sovereign-internet/



3. PROTECT THE FORCE

In the future IW threat landscape, it will become even more imperative that the DoD invest and discover new ways to protect its service members from external manipulation. The Information Warfare Framework can help to deconstruct the potential for conflict in the three domains (digital, cognitive and physical). From there specific actions can be taken to make the force aware of potential and possible attacks, especially when deployed. Protection measures will vary and need to be modified depending up what portion of the IWF three domains are attempting to be addressed.

Potential Actions:

- Implement regulations, training, or specialized/isolated information networks.
    - ◊ With the deluge of information available outside these proposed enclaves is overwhelming and impossible to contain.
    - ◊ Control is much tighter inside the DoD information space, at the risk of shielding our service members and families from alternate points of view contrary to DoD policy.
    - ◊ Understand that ultimately there is no way to implement full control on global social media
    - ◊ Expanded training and measures to support family members of force who will also be targeted
- A concerted government regulatory effort must be made to convince social media companies to develop a strategy to disrupt, mitigate and deal with the affects of fake and inflammatory content. Regulatory efforts need to be developed that encourage economic incentives for creating open platforms that simultaneously balance freedom of speech and privacy concerns.

4. COUNTER THE TIDE OF SOFT POWER

Soft power *n. power (of a nation, state, alliance, etc.) deriving from economic and cultural influence, rather than coercion or military strength*[25]

Although technology solutions such as algorithms that detect deep fakes or discover social media manipulation will be necessary and vital to understanding the fight for truth, people are often better at verifying truth with their own senses. But we also must remember that these senses can be easily tricked without alternative information sources.

Potential Actions:

- Employ Human-cyber teaming systems that can be more acurate than either humans or algorithms alone
- The future of conflict will be informational and the DoD must consider moving away from its heavy reliance on kinetic strategies in the physical environment.
- Beating the growth of China's soft power approaches in Africa requires competitive alternatives to Chinese products and military strategies that lead with information warfare.
- The US will require a "whole of government", "whole of society" and possibly "whole of western democracies" strategy to counter informational attacks by state and non-state actors against our nation and its institutions. However, the US does not need to adopt strategies that use deceitful techniques, such as lies or deep fakes content.

5. DISRUPTION & DELAY STRATEGIES

Military strategies of disruption and delay are not often favored as the first choice when developing responses to adversarial actions, but what the US currently needs is time for governance, research, and values to catch up with the speed of technology.

A potential action could be to explore disruption and delay information strategies that the military can implement while diplomatic, economic, and other whole-of-government approaches tackle the long game.

[24] Cheung, E. (2020, Jan 8). China bans foreign teaching materials in public schools. CNN. Retrieved from https://edition.cnn.com/2020/01/08/china/china-schools-foreign-ban-intl-hnk-scli/

[25] Oxford English Dictionary

FUTURE THREAT INDICATORS

Analysis of the raw data and emerging themes from the three IW Threatcasting workshops revealed a number of threat indicators for IW and the future of conflict.

One unique set of indicators spanned many scenarios in which cultural belief systems were used as a new manipulation device. These belief systems helped to drive individual and group actions with nearly automatic decision making and neuro-prioritization allowing people to be manipulated across and regardless of geographies, affiliations or beliefs . By manipulating information that directly relates to cultural belief systems, or decisions based on cultural belief systems, bad actors gain unprecedented access to the psyche of intended targets – not only impacting immediate behavior but longitudinal outlook as well. Many of these implications are interrelated, and can be combined to create networked implication systems affecting lay citizens and military personnel alike.

Definition: Flags

The Threatcasting process 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"[26] 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. It remains unsolved how best to monitor them at scope and scale.

[26] Webb, Amy. The Signals are Talking: Why Today's Fringe is Tomorrow's Mainstream. PublicAffairs, 2016.

FLAGS

The implications from the IW findings reveal a palette of flags, or events and realized situations,identified directly and indirectly from the threat future data that gave us specific areas to progressively monitor for possible threat futures. Marshall et al. proposes that the progression of disorder is always subjective and therefore, the flags that forecast the imminent threat, may also be subjective.

The following flags are grouped into specific areas or domains so that these can be monitored for indicators that the flags have happened. These categories are designed to help practitioners utilize and apply the flags to their work. They are not meant as a definitive classification. In fact, many flags can be categorized in multiple domains. Each of the flags below are micro-indicators that the threats outlined in this report are being to emerge. Often the flag will build off each other, giving the DoD multiple early stage indicator to prepare for the threat.

SOCIAL

- Increasing opacity of algorithms directing people's behavior in real life, and a decrease in corporate desire for transparency
- Biometric measurements become standard procedure for identity verification (voting, internet usage, monetary transactions, etc.)
- Credentialing of internet of things (IoT) device information sources (accredited media) started to be used to counter dis-, mis-, and malinformation
- Free speech is continued to be privatized to the point of intellectual and cognitive "solitary confinement"
- Continued split of communication channels along cultural, partisan, geographic and ideological lines
- Emerging reliance on immersive technology (AR/VR/MR) as communication dissemination platforms
- Growth in pro-Chinese messaging in the local environment along with information environment observation of pro-China shaping of the global stage
- Increasingly unethical use of technologies in novel ways; troll farms, deep fake content production (disinformation)
- Adversarial media outlets develop narratives that counter reality and support their national influence campaigns

- Governmental imposition of free speech limits on media/data companies

TECHNOLOGICAL

- Emergence of automated (AI driven) deep fake generation
- Evidence of successful low level deep fake attempts, integrated into the operating environment
- Emergence of automated information distribution capabilities making attribution more difficult
- Increasing targeted advertising, specifically involving political recommendations via search engines, ads and social media
- Increasing opacity of the algorithms directing people's behavior in real life, and a decrease in corporate desire for transparency
- Increasing interoperability of platforms and systems - both military and civilian
- Exploitation of neutral gaming systems for messaging (emotional connectivity through gaming platforms)
- Emergence of human body implanted augmentations that translate digital information and are capable of generating physical/psychological effects
- Development of AI/ML with unconstrained access to global data by an authoritarian organization or government –
- Increasing lack of viable alternatives to Chinese owned information and communications technology providers in Africa
- Expansion of the great fire wall to include nations that adopt, purchase or accept information technology infrastructure with specific focus on the expansion into social netowrks and computing
- Global expansion of Chinese owned networks that compete/replace other western networks
- Reliance upon Chinese owned networks by underdeveloped countries within their Belt and Road Initiative (RBI).[27]
- Ability of Natural Language Processing to map regional and cultural dialects. Elimination of cultural clues and errors in speech.

ECONOMIC

- Foreign technology companies gaining access to and winning market share in the US (e.g. Huawei)
- Investments by both private and public sectors in media and data literacy
- Creation of an explicit data market
- Increasing influence of China's Belts and Roads Initiative (BRI) using foreign

[27] Cai, Peter. "Understanding China's belt and road initiative." (2017).

national debt for leverage and influence (e.g.Venezuela and Sri Lanka[28])

- Foreign nations begin to build alliances and partnerships for technological or security motivations that then influences broader domestic actions (e.g. China outspends, Russia out arms)
- Example: China lends capital and technology for infrastructure projects and then uses Chinese labor over local labor
- China able to gain economic control in host nation through long term loans for infrastructure projects based on the price of host nation's commodities
- Reduction in funding and manning for the Department of State and other diplomatic engagement tools.
- Increasing Chinese control over natural resources and population information control
- Black market that operates outside of Chinese social credit system. Characteristics could include digitally segregated or analog or a hybrid. Initial emergence on the Dark Net

ENVIRONMENTAL

- Destabilization from climate events continue and broaden
- Extreme or heightened urbanization
- Increased division in ideologies between urban and rural environments

POLITICAL

- Degradation of political action oversight ("the law doesn't apply to me")
- Shift or Drift in the rule of law
- Local laws gain more support than national or constitutional laws
- State constitutions override federal decisions
- Campaigns that focus of regionalism (e.g. Cascadia, Jefferson state)
- Specific calls for states or region to secede
- Establishment of an anti-democracy party within the US
- Proxy battles between nation states increase in the information realm (e.g. Russia using Ukrainian separatists to attack the legitimate Ukrainian government enables plausible deniability)
- Increasing domestic (USA) terrorism that sees fewer lone wolves and more groups or organized cells.
- Formation of new international conglomerates (Mexico / China / Russia)
- Increasing misinformation campaigns

or political communication focused on countries

- Changes in country's information warfare strategies.
- Example: Changes in Hong Kong strategies could indicate future techniques, tactics, and procedures
- Global Ideological Shift: Chinese whole of nation approach gains prominence as opposed US separation between political and economic agencies/institutions
- Increasing legal/regulatory limitations on data operations within US/targeted to US Citizens

MILITARY

- Increasing adversary ability in space that leads to increased control over ground level perspective
- Emergence of Chinese willingness to use proxy forces, providing information to lethally attack US forces
- Increasing Chinese force projection capabilities with increasing presence and capabilities outside of mainland China
- Increasing insider threat behavior
- Increase of non-discriminate targeting of families / soldiers - mission distraction
- Increase of discriminate targeting of families / soldiers - create polarization in forces
- Increase of adversarial deception operations through social media and tech applications
- Adversary begins to collect and attack units and leaders at the tactical level to include individual and personalized targeting
- Spread of a culture of willful ignorance inside the military, moving away from shared understanding of virtues and vices

[28] Brautigam, Deborah. "A critical look at Chinese 'debt-trap diplomacy': The rise of a meme." Area Development and Policy 5.1 (2020): 1-14.

POSSIBLE ACTIONS

(DISRUPTION, MITIGATION AND RECOVERY)

The Threatcasting Workshop uncovered not only threats and flags but also actions that could be taken to help mitigate, disrupt, and/or recover from the threats. These actions constitute a "whole of society" approach to problem-solving and have been applied to specific domain areas where detailed steps can be taken. All these actions must be fluid to adapt and shape the future applications of technology. As soon as a stopgap or detection protocol is created, adversaries will work on ways to defeat it, so there must be dedication to continued monitoring and analysis. These actions illustrate that IW threats are not solely due to the incremental changes in the expanding technological attack plane. These IW threats will require fundamental psychological, cultural, and institutional changes.

The following categories are meant to give clarity for who can take specific action to disrupt, mitigate and recover from these potential threats. Because these threats are a whole of society problem, it will be important that all sectors and domains work together and collaborate.

"WHOLE OF SOCIETY" SHARED ACTIONS

- Recognition that the future of Information Warfare will target free speech as a specific vulnerability, making the threat to the "whole of western democracies"
- Invest in early data and media literacy across levels of influence in both the private and public sectors
- Investment in detection of falsified, fake, and misrepresented news items including networks and social media platforms
- Investigation into advanced data privacy requirements

MILITARY / GOVERNMENT

- Credential troops and government employees to distinguish between fake and real content (audio, video, and narrative) and to understand algorithmic decision making
- Develop explicit expectation management of the training benefits

of emerging technology in training environments. Research, recognize and understand the potential shortcomings of our service members in the usage and manipulation of these technologies

- Decisive investment in US state-sponsored AI development in tandem with ethical AI standards development
- Develop ability to detect 5G mobile ad hoc mesh networks
- Establish an Information Warfare "Geneva Convention" in order to identify and address emerging threats on a global level - redefine the Laws of War
- Unify language in the political discourse – unifying American narratives need to be crafted and socialized

ACADEMIA / EDUCATION / PHILANTHROPIC

- Fund studies on the psychological impact of AR/VR/MR technologies on human beings
- Invest in research that identifies effective tools and education for increasing digital literacy that can be handed to non-profits for dissemination (à la international aid currently)
- Establish grants to support local investigative journalism, understand emerging technology networks, and psychological vulnerabilities based on citizen data exhaust
- Explore the intersection of data viruses and biological viruses to better understand plausible breakdowns between the digital/biological barrier

INDUSTRY / TRADE-ASSOCIATION / NON-PROFIT

- Fund efforts to create dedicated intrusion detection within the VR environment
- Convention between big tech and government on ethics in media framing and information dissemination systems
- Develop pervasive AI-enabled scanning of networks for intrusions and hacks

CITIZENS

- Exert effort in self-monitoring data exhaust by questioning the terms of service for each data, service, and digital product provider
- General awareness and hardening against psychological manipulation specifically via digital media
- Become informed data citizens, parents, teachers, educators, and students
- Understand the intentions and designers of systems and gamification services to become more aware of psychological influencers

OPERATIONS SECURITY (OPSEC) ANALYSIS

Where Critical Information, Threat, and Vulnerabilities Co-Exist

This section describes another way to consider the value of these threat futures by asking what information, norms, values, and societal structures they actually attack, and whether we are actually vulnerable in the areas identified in this research. If we need to protect something but there is no avenue to reach it, or if the threat does not have the capacity to get at our protected item, there is no need to apply resources against the threat itself. As we consider this threat-vulnerability connection, we must make certain assumptions about the things we are trying to protect in the future of IW.

The following are a few of the important things we assume information warfare protect:

1. The U.S. Constitution and democratic processes are non-negotiable "good" values that should not be changed except through established venues. These processes themselves can be changed by the legislators with the consent of the governed. The vulnerability becomes the governed themselves, evidenced, for example, by the Russian assault on democratic processes in the 2016 presidential election.

2. Democracy itself is a beneficial form of governance that is worth protecting, not just from the American point of view, but also from an international cooperation perspective. The vulnerability becomes international credibility towards the American form of democracy or whether a different type of governance can just as easily satisfy the needs of a population.

3. Human Rights. Although the U.S. subscribes to the Universal Declaration of Human Rights (UDHR) as ratified by the United Nations in 1948, it is an international treaty that is not technically binding in the US unless there are federal, state, or local laws making a right explicit (sometimes a court decision or interpretation can give a right legal status). According to the Advocates for Human Rights, the Constitution does not provide for many economic, cultural, and social rights that are inherent in the UDHR.[29] We might assume that most human rights are protected values, but it is not safe to say, in the context of this framework, that a U.S. response to an IW threat would protect all rights as outlined in the UDHR. Thus, there could be a vulnerability in the relationship between the U.S. perspective on human rights and the perspective of the UN.

[29] www.theadvocatesforhumanrights.org

4. Balancing the primacy of the state versus the primacy of the individual. For instance, if a legislator proposed a law that said, "in order to prevent the spread of automated bots, social media companies must 'know your customer' and implement some way of positively identifying a real person behind the keyboard," that might come into conflict with the individual's expectation of anonymity online or even expected right to privacy. Conflict between these different perspectives could indicate a vulnerability that can be attacked using IW techniques.

5. Critical Infrastructure and Key Resources (CIKR). According to the DHS website, CIKR are the "assets of the US essential to the Nation's security, public health & safety, economic vitality, and way of life. Simply put, its power grids and water filtration plants; national monuments and government facilities; telecommunications and transportation systems; chemical facilities and much more..." CIKR are often privately owned and thus requires a public-private partnership and high integration to effectively & efficiently protect. The relationship between public and private, state and federal control over CIKR, and the balance of resources required to defend CIKR might constitute a set of information vulnerabilities adversaries could attempt to exploit.

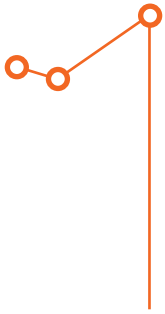
6. U.S. hegemonic power. Is economic, military, or political supremacy around the world an existential value worth including in the long-term IW battlefield? Being the top of everything may have its perks, but also requires a tireless vigilance that is expensive and cumbersome to maintain. Any number of long-term strategies that distract attention from national goals to stay ahead of the rest of the world take away resources from actually achieving those goals.

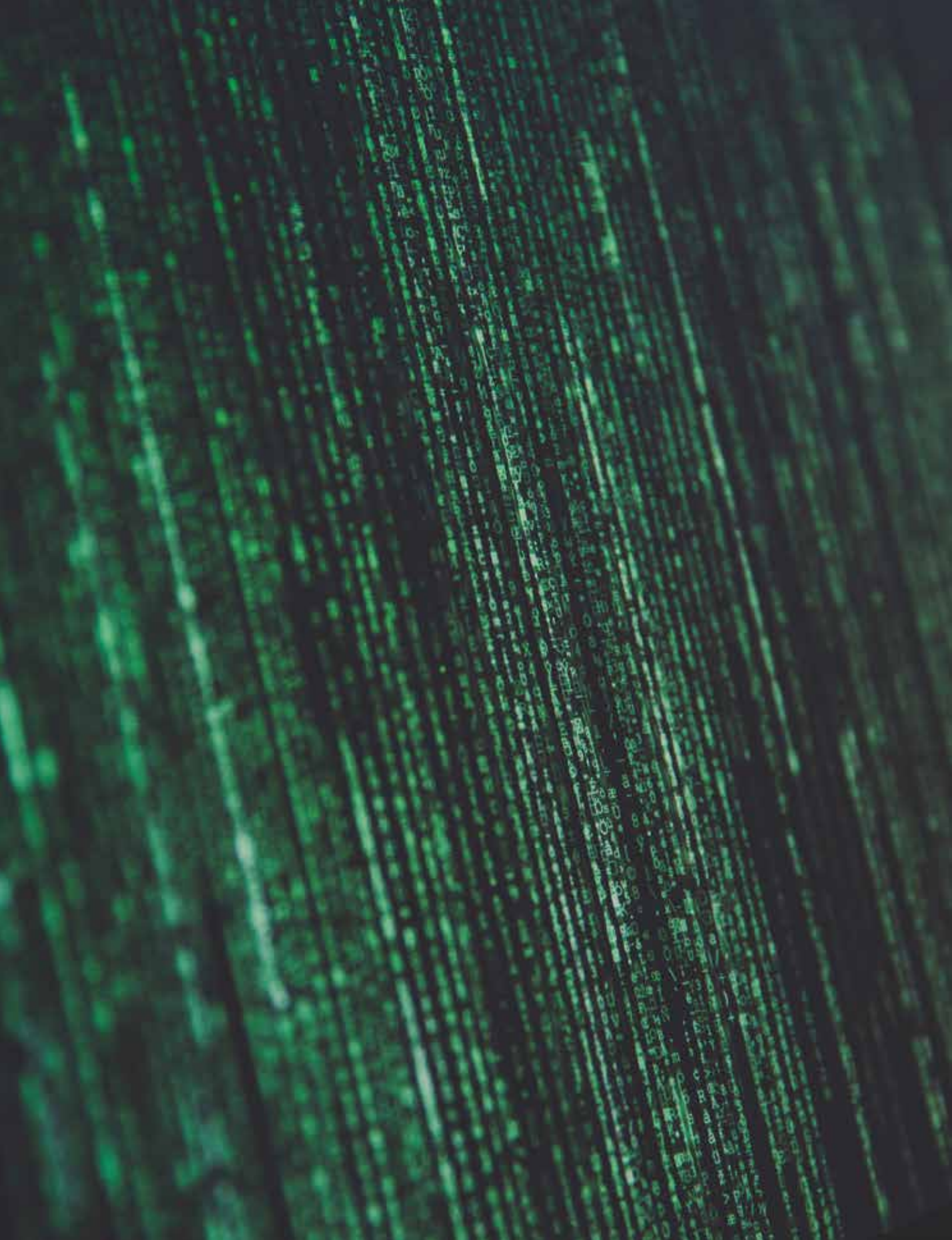
7. Vulnerable populations. Current events and current policies have shown that only those vulnerable populations that are able to fuel certain political thrusts or agendas are at the forefront of the IW battlefield. Those vulnerable populations that are not on the current political agenda may not receive any special consideration in the future of IW.

Once we understand more fully what elements we are trying to protect –the "objects" of IW– then we can move forward to analyzing how IW threats can exploit particular vulnerabilities and how we can apply resources to shrink vulnerabilities or the impact of threats against them.

[30] https://www.dhs.gov/blog/2009/11/19/cikr

APPENDIX
TABLE OF CONTENTS





APPENDIX A

INFORMATION DISORDER MACHINES[31]

WEAPONIZING NARRATIVE AND THE FUTURE OF THE UNITED STATES OF AMERICA

In the coming decade, advances in technologies like artificial intelligence (AI), machine learning (ML), quantum computing, the internet of things (IoT), smart cities, and autonomous vehicles in land, sea and air will enable adversaries of the United States to mechanize information disorder to influence, manipulate, and harm organizations and individuals. These coming information disorder machines (IDMs) will be targeted broadly at groups and geographies. AI and ML will allow for increased if not complete automation, allowing IDMs to adapt in real-time down to the individual level, creating personalized attacks while operating at a mass scale. The emerging threat of IDMs lie in the unique pairing of their real-time microtargeting and the macro effects that can have at scale. This is a direct threat to national and global security as well as a threat to the future of the United States of America.

Future Threats:

Adversaries use IDMs to incite violence and tribalism, encourage anti-federalism, inspiring populations (regardless of political affiliation) to question the authority and relevance of the United States government and the union. This destabilization will distract populations, governments, and militaries, focusing on inflamed issues so that other adversaries can gain advantages elsewhere.

Generally, adversaries will exploit desperate conditions or catastrophic events to sow unrest and inspire mistrust in traditional organizations and governments, ultimately encouraging individuals to move to violence.

Adversaries (foreign and domestic) will use IDMs to incite public outrage and destabilize entire business areas (e.g., technology, medical, education).

Domestic extremists and terrorists will use IDMs to further their domestic agendas, causing harm to individuals and destabilizing organizations.

Corporations will use IDMs to increase profits, reach, and competitive edge while causing harm to individuals and each other.

Domestic businesses as proxies for foreign adversaries will employ IDMs to target and harm citizens, steal intellectual property, and destabilize the United States.

Citizens and special interest groups (nontraditional adversaries) will use IDMs to weaken the union of the United States, the education system, and the strength and resiliency of society.

IDMs will weaken belief and participation in the military and education systems,

making the nation vulnerable and less competitive globally.

Possible Actions to be Taken

The IDM Threatcasting Workshop also identified a range of possible ways to disrupt, mitigate, and recover from the threat of IDMs. These actions span across multiple domains including government, military, industry, trade associations, academia, and average citizens. A single organization cannot meet the threat of IDMs; over the next decade, each domain will need to learn to inform, collaborate, and support the others.

Business, governmental, and public recognition that IDMs are a threat to economic stability and national security. The cultural conversation about IDMs exploitation of the worst of ourselves against ourselves.

Development of technologies to detect, uncover, and attribute the use of IDMs.

Support of watchdog organizations to detect IDM activity and the conditions under which they will thrive.

[31] Johnson et al. Information Disorder Machines and the Future of the United States of American. 2019. http://threatcasting.com/wp-content/uploads/2019/10/threatcasting-2019-w-footnotes-PRINT.pdf

APPENDIX B

OVERVIEW OF SUBJECT MATTER EXPERTS

This workshop relied upon the expertise of nine specialists from academia, industry, technology, and security. These subject matter experts provided the context, settings, and an idea of future trends for marketing, advertising, cyberwar, information operations, Russian security studies, technology, and science fiction in the future of information warfare. Some experts have chosen to remain anonymous in this report.

Brad Allenby, President's Professor of Sustainable Engineering, and Lincoln Professor of Engineering and Ethics, ASU

Some of the scenarios we may encounter in the next decade will be such novel exploitations of previously unseen cracks in our fundamental beliefs, values, and processes, that we think they "sound ridiculous today" to even consider them. But that's exactly why we are most unprepared; we have taken these "Democratic institutions" for granted since we settled the matter of the U.S. Constitution. The "variety, the velocity, and the volume of information" is creating swift currents that are "overwhelming existing institutions" and "overwhelming many people."

Anonymous, Chief Creative Officer

One of the subject matter experts succinctly summarized our relationship with marketing and media with the following statement: "Culture is in a constant state of inflammation. Media is the active agent that's firing that inflammation." Much of this inflammation is due to the "attention economy" of marketing and the fine line between advertising and manipulative propaganda. Many people love to be at the center of attention, at least for a time, yet the sophistication of marketing allows everyone to always be at the center of their own world, and there is no shut-off button, no rest from being at the center. This has turned "people into [a] product to sell to advertisers." Marketing media has been complicit in the inflammation of many social ills such as objectification of women, "creating problems that don't exist so that you can buy more stuff," reinforcing "a constantly receding ideal to strive after," and the monetization of digital addiction. When the attention of so many people has turned inwards, who is left to look outwards?

Anonymous, Chief Data Scientist, Fortune 100 Company

In the future, a hyper-connected world may see conflicts begin and end at the speed of electrons and it may be fought by algorithms opposing other algorithms. This requires an information warfighter that is "data literate at every level." This will likely require the "development of new institutions and the reshaping of existing institutions" focused on training warfighters to "merge augmented, virtual, and physical realities" and being comfortable using artificial intelligence tools in a responsible and ethical way. Several obstacles exist that could hinder our ability to develop warfighters of this type: gaps in education, income, equality, and emotional intelligence may impede the ability of the United States to participate in the future arena of international competitiveness and cooperation. "What's difficult is that there is no existing playbook to these challenges around privacy,

cyber warfare, open source data, use of social media data, and the moral conundrums associated with artificial intelligence."

Anonymous, Marketing, Advertising, and Business Intelligence Expert

In the future, people will still get their news fix, but a shift away from print, TV, and radio news will accelerate as the population ages and consumers gravitate towards sound bites, headlines, and filter bubbles delivered by automated systems on their social media app of choice. This means that news of local importance will decline and will be reduced in quality and depth as fewer outlets will cover "regionally specific issues." Fake news, active disinformation campaigns, and click-bait headlines will continue to increase as they are effective in filling the 280-character attention span of the modern consumer. What is still unclear is the role media providers have in monitoring, policing, and changing policies around "acceptable content distribution." Much of the burden may fall towards content providers in filtering fake and contrived news, since there is still a dearth of investment in media, data, and truth literacy.

Anonymous, Russian Warfare Expert

"Manipulation," "Influence," "Persuasion," and "Propaganda" are several terms that describe the idea of reflexive control, or getting someone to do what you want them to do. Oftentimes, getting another person to change habits and behaviors incites a little bit of chaos in that person's life as they struggle to adjust to new ways of thinking or new practices. Instead of thinking of the new habit or behavior as the goal of information warfare, there are adversaries and potential adversaries who may have the goal of simply increasing chaos and disorder. For every moment thinking about how to "counter" an adversary's message or return to the status quo, that is a moment not spent on achieving one's own goals, and a little bit of chaos is created. Multiply those moments by the speed of hyper-connected and automated systems, and the amount of chaos grows wildly, as does the amount of effort required to "rebalance" the system. Except there's a catch: the status quo - the balanced system, or at least one that favors U.S. ideals - is actually a system of increasing disorder. For example, Russia sees truth as a moving object and they are quite comfortable with multiple versions of the truth, depending on what is convenient at the time. This allows for more convincing deception operations, especially those augmented with better tools to fake and shape the realities they display to the world and to their own population.

August Cole, Author

Just as Threatcasting is a tool to systematically consider possible paths to possible futures, it also gives people the opportunity to shine a little bit of light ahead into the darkness; In a sense, foresight methods help us plan for and build a view of the future that is preferable to those doing the planning and building. There are emerging tools that allow other people to plan for and build their own view of the future. The first way is by leaning on VR/AR/MR, video and audio manipulation, automated content generation, and fundamentally unique ways of thinking to generate altered versions of the present, which gives everyone a different starting line to begin the race to the future.

The second way is to bend and rewire relationships between public and private concepts of information. This includes various interpretations of privacy and data ownership, novel uses of data captured while online or through wearable devices, and concepts of power shifting

because of the type and volume of information that is public or private.

The final way we might struggle with others building their version of the future is in the way we ride the wave of experimentation, training, and ethical boundaries of new technologies. One subject matter expert poses this question: "What is the information domain equivalent of banning cluster munitions, where would such a concept be applied, and which countries would abide by an agreement?" Those who are currently experimenting with the power of hyper-connected information to influence and shape realities may be the ones least likely to agree to some sort of controls over that power, yet may be the ones most in need of boundaries.

Cyndi Coon, Threatcasting Lab Chief of Staff

Information Disorder Machines, or IDMs, are those fully- or mostly automated functions of information manipulation that can connect each person with the right message at the right intensity to influence the masses and potentially cause tremendous harm. Elsewhere in this report, we find that IDMs play a central role in moving along the social and cultural waves of change that incite violent actions, swing mighty blows at democratic values, and inspire populations to "question the authority and relevance of the United States government and the Union." Corporations may use IDMs to move along waves of brand popularity while simultaneously attacking competitors' credibilities or trust with consumers.

Herbert Lin, Senior Research Scholar at the Center for International Security and Cooperation; Hank J. Holland Fellow in Cyber Policy and Security, Hoover Institution

Cyberwar and cyber-enabled information warfare are siblings that share parents but are unique enough to discuss them separately. Cyberwar takes "advantage of the flaws in information technology and design of implementation" and is in conflict with computers, data storage, and data transfer. Information warfare takes advantage of the "vulnerabilities in the human mind" and is in conflict with decision making, thought processes and the "views, attitudes, and behavioral predispositions with respect to other people, institutions, [and] nations." With increasing frequency, cyberspace operations unlock previously concealed or hard-to-access avenues for information operations to be successful. These "sibling" operations will enable the information warrior to use an environment of "high connectivity, low latency, anonymity, and inexpensive production of information" to focus targeting, increase receptivity to messaging, and "give large megaphones to what formerly were fringe players."

Harper Reed, Technologist-Entrepreneur-Hacker

Just as it took decades of climate research to understand the pollution effects of internal combustion engines, we are still only in the beginning stages of understanding the negative effects of our digital and social exhaust. Every digital device, especially those connected to the Internet and cellular networks, leaves a constant trail of activities, behaviors, preferences, signatures, and connections - both for the device and for the user. A lot of people are not even aware they are spewing forth all this data, which is why exhaust is such a good word. Savvy companies are scooping up every bit of this digital exhaust, re-purposing it for good and for ill, and there are very few controls about how to manage or even understand the scope of this problem.

APPENDIX C

SME TRANSCRIPTS

Allenby_Future of IW (transcript), 5 Sep 2019

Threatcasting and the experience we've had with information Warfare in recent years particularly since 2016, I think there's several trends that are worth thinking about.

First is that we need to be very broad in the scenarios that we consider. If you think about for example, the fact that in October of 2016, Netflix on its Black Mirror sci-fi program, introduced the idea of social credit systems and a year later and a year later China was rolling it out. It indicates that the timeframe of technological evolution has collapsed.

That means that if you want to think 10 years out you need to think in terms of really difficult scenarios. Scenarios that sound ridiculous today, not because you think necessarily they're going to come true, of course, but because we need to be able to broaden our thinking to handle things that are far different, because of the speed of technological evolution, than we might have thought before. So that's one thing.

The second thing is, by and large, the immediate immune response of American and European systems to things like the Russian disinformation campaign has begun. NATO is looking at it; the Baltic states, of course, are very concerned about it; The U.S. is looking at it. That needs to continue, but we also need to understand that that's not sufficient.

There are two tracks here that we need to work on simultaneously. The first is the immediate immune response: what do we do, for example, when Russia begins combining Cambridge Analytica-type activities with CGI and voice technology in the 2020 election?

That's the kind of thing we need to be thinking about immediately, but that short-term. We also need to think about the institutional implications, longer-term, of the kinds of changes that we're seeing in the information environment.

For example, it appears at least arguable that issues of free speech have now become privatized. At the terms and conditions of social media companies like Facebook Twitter and YouTube have as much to say about free speech is anything that American courts decide.

It also looks as if the pluralism and diversity which has been a strength of the American system is now becoming an exploitable weakness targeted by our adversaries.

What does that mean? Now, I want to emphasize it doesn't mean that the values are wrong, but it does mean that we need to be prepared for fundamental attacks on Democratic institutions that we have taken for granted for 200 years. And that we are not prepared to do. So that's a significant weakness.

If you're doing an overview of the democratic West, the Europeans and the Americans, then one of the questions that we need to be asking that we haven't asked is what fundamental weaknesses are exposed by this increasingly rapid acceleration in the variety, the velocity, and the volume of information? It's overwhelming existing institutions, and it is certainly overwhelming many people.

What are the implications? We haven't begun to think of that and yet, that in the longer-term, may prove to be the fundamental weakness that undermines Democratic systems and favors soft authoritarianism.

Anonymous, Chief Creative Officer, Future of IW (transcript), 9 Sep 2019

It seems we're in a time when short-termism and extremism are holding hands to make emotional liability the norm. Culture is in a constant state of inflammation. Media is the active agent that's firing that inflammation. We all talk about it but I'm not sure we're really taking into account where this could go. We discount it. We assume only "people less smart than us" are affected by it.

You don't have to look further than what we did for Nike and Colin Kaepernik to see what manipulation of emotional mass reaction can do.

Friction creates heat. Heat creates energy. Energy transforms things.

Make America Great Again.
The Democratic Socialism of Bernie and Ocasio-Cortez.
Times Up.
Black Lives Matter.
March For Our Lives
Youth v. Gov
#TrialoftheCentury

None of these are advertising campaigns but they all use the tools of advertising.

Marketing media has been weaponized.

Take this example from the headlines this weekend:

"Days after Sudanese soldiers massacred pro-democracy demonstrators in Khartoum in June, an obscure digital marketing company in Cairo began deploying keyboard warriors to a second front: a covert operation to praise Sudan's military on social media.

The Egyptian company, run by a former military officer and self-described expert on "internet warfare," paid new recruits $180 a month to write pro-military messages using fake accounts on Facebook, Twitter, Instagram and Telegram. Instructors provided hashtags and talking points."

The line between advertising and propaganda is a fine one. Adding detailed personalized data to the mix pushes us over that line.

We all know this peripherally. But I ask you to consider the way this works:

We, in the attention business, are complicit in a long and shameful history.

You can read all about it in Tim Wu's excellent book, The Attention Merchants.

Turning people into product to sell to advertisers. Complicit.

Benjamin Day, founder of the New York Sun, invented this business model 170 years before Facebook or Google weaponized it.

Feeding the British war machine of 1914 which sent an entire generation of young men to the slaughter. Complicit.

Creating the propaganda machine of the Third Reich, which was modeled on the British propaganda machine of WWI. Complicit.

Creating problems that don't exist so that you can buy more stuff. Complicit.

Surfacing your subconscious anxieties - "All around you people are judging you silently" - Complicit.

Giving people, particularly women, "a constantly receding ideal to strive after." Complicit.

Objectification of women. Complicit.

To take that one step further... Complicit.

Reinforcement of negative racial and gender stereotypes. Complicit.

Addicting millions of people to tobacco. Complicit.

Monetization of digital addiction. Complicit.

The rise and dominance of the Four. Definitely complicit.

I cringe when I read that "Unilever has an ambition to have a billion one-to-one relationships."

Targeting. This is the solitary confinement model of marketing. If only one person can see something, the potential for abuse is high.

I wonder if one simple rule could pull you back from potential social catastrophe: all advertising must have witnesses.

When you watch the unbelievable things happening in the world on a daily basis, this period of rapid change and developments. Automation of our workforces, climate change, forest fires, mass shootings, the resurgence of white nationalism. It can be very hard to discern what's real and what's not anymore.

So, I don't just look at data privacy when I look askance at the trajectory that advertising is taking. I worry about what mass, targeted disinformation and emotional manipulation could do to culture. I worry that we are a powder keg waiting to explode.

If the current trajectory of persuasive media, unchecked, incredibly difficult to regulate, thriving in shock and outrage...what is the threat? Is it worth the value of the attention economy we have created? Can it get worse? I think so.

Anonymous, Chief Data Scientist, Fortune 100 Company, Future of IW (transcript), 7 Sep 2019

I'm [redacted] happy to participate in this Threatcast for the Army and ASU, focused on AI-enabled Warfare 10 years from now.

I'm speaking to you as a scientist, an independent researcher, and academician and I'll focus on three main areas.

The first is managing data in a fully connected state. 10 years from now we will see that artificial intelligence is very different from any of the other technologies we've ever used on the battlefield, asymmetrical or otherwise.

The technology will be focused on a fight not between just military soldiers, [with] bullets and missiles, but more specifically data vs. data, AI algorithms versus AI algorithms. And this will happen in a fully connected, converged state where all data, sensors, the Warfighter, space -- all of the environment and all the technologies that support the IT environment will be fully integrated and fully connected.

This will have a significant impact on the structure and integration associated for strategic advantage over an adversary not like the least of which is focused on cyber warfare and adversarial machine learning or deep learning.

But it does highlight a very serious gap in terms of data literacy. We need to find ways to make the warfighter data literate at every level. The ability to harness the power of data and be able to apply it in every battlefield situation would be a key advantage and being able to understand how to close the gaps associated with data literacy in war fighting is going to be a significant activity.

Second, is this idea of international competitiveness and cooperation. Clearly there's a question about if, well, other nation-states are participating in the use of artificial intelligence-enabled warfare, what are the boundaries or guidelines that the United States ought to position itself into?

Well, in 2030, this question will be enhanced with an understanding that military superiority in the United States will have vanished and so there won't be any gap between us and our adversaries' ability to wage an algorithmic, AI-enabled warfare, and this will lead us to deal with some very significant non-technical issues that would improve and enhance our competitiveness and the use of AI.

First is the gap we have in education. In 2030, we will no longer be able to operate in a situation where we have people who are meeting or receiving varying levels of education. We would need to close the inequality gap around education so that we have active participants not only from a war fighter perspective but across all areas of the civilization.

We will need to focus more attention on the income gap and the inequality in income and wealth. It's going to be important because we want full participation and we're going to require full participation of all people in our civilization in our country in order to meet the challenges associated with AI-enabled warfare 10 years from now.

And probably one of the things we need to emphasize is this refocus on data literacy, not just in terms of the data literacy of the Warfighter but data literacy of the citizen data scientist. We can no longer afford in 2030 a situation where citizens do not know how to harness the power of data to achieve an outcome.

And it will raise some significant questions around what kinds of institutions you want to have, both in the National Security community, but also in the community-at-large. By focusing on innovation in 2030, there would be a convergence of biomimicry and bio convergence with advanced computing as well as a new focus on cognitive enhancement so that we can do more neuromorphic capabilities and learn in unusual ways outside of the programming we have in our current narrow AI.

It will require the development of new institutions and the reshaping of existing institutions.

As the virtual and physical spaces in which we operate merge, augmented, virtual, and physical realities will become much more than a gaming platform. What they will actually become is a Global Communication platform for all our operations including military battlefield operations, medical, and language skills at the battlefield edge, and the ability to gain a competitive Advantage from a data perspective.

Last is the responsible and ethical use of AI. And as human enhancement via artificial intelligence continues to grow, as we continue to unlock the human genome and find ways to enhance human strength, sight, hearing, speed, we will put stress on the military policies and ethics that guide the use of artificial intelligence. And years from now we'll be asking ourselves more about whether we should do something as opposed to whether we can act.

There would be a significant focus 10 years from now on our ability to grow emotional intelligence just as much as it is on artificial intelligence. And the United States will have a clear understanding of whether or not it wants to be part of that entanglement with its competitors or adversaries or a disentanglement strategy with its adversaries when it comes to AI-enabled warfare.

The challenge is the lack of an existing playbook to these challenges around privacy, cyber warfare, open source data, use of social media data, and the moral conundrums associated with artificial intelligence.

So I'm excited that we'll get a chance to review the work from this committee and I look forward to seeing the outcome in the report.

Anonymous, Marketing, Advertising, and Business Intelligence Expert, Future of IW (transcript), 8 Sep 2019

Hello, I'm [redacted]. We're the world's largest buyer of advertising representing many of the world's largest advertisers. We deploy around 48 billion dollars a year on advertising, paid media, primarily, but also work with marketers across a wide range of their marketing needs. And [inaudible] with the rest of our [redacted] siblings, offer a comprehensive range of marketing services.

I am a former securities analyst covering stocks associated with the advertising industry. Before that, I worked for an advertising technology company. Spent another eight years working for another holding company in a similar role. And before that was an investment banker and analyst.

In this role, my job is to help our clients, our agencies, our parent company, think about the future, help to set the agenda for issues that matter, or should matter, to all of them, and in doing so, produce a wide range of research, which you can access via our website at GroupM.com, or you can reach out to me directly if you'd like to receive that in the future.

I was asked to speak about the future of information and campaigns. For starters, it's safe to assume that consumers will access content and information with increasing frequency, in digital media, in digital environments in varying forms. That primarily means social media apps, unconventional news publications, [and] other digital platforms, whether apps or websites. That trend is just continuing; it doesn't seem to be any reason that lets up.

Television and radio will still be very important. They still are a critical source of information for a wide range of consumers, especially for older consumers, but they will diminish in their relative importance as time progresses, in terms of reaching out to a broad range of the population.

Word of mouth is something that sometimes doesn't get thought about a lot because there's no money going to it, or very little money applied towards word of mouth. But keep in mind that that's probably one of the most important ways that information has always been distributed and always will be distributed. Really amplifying information delivered through other means initially.

As we think about other ways in which information can get distributed, certainly immersive digital experiences are increasingly likely to be common. Virtual reality, augmented reality, are probably the ways we characterize it today. All of this enabled by widening availability of faster broadband speeds. 5G is sort of a by-word for this, in context of communications. But the idea that it will be easier to receive substantially greater volumes of data, seems very likely to be a widespread thing -- that most people will have faster broadband, and therefore more immersive experiences will be possible, and that will be increasingly important for all forms of information distribution. None of the aforementioned types of content distribution go away, but they will evolve in terms of their relative importance.

Now, challenges to how information is distributed will expand. Many of these we see today in different forms, and they'll just continue to evolve best as we can expect. Maybe the first item to hit on is the idea of the "news desert." Journalism has really been hollowed out over the past two decades as traditional print publishers failed to adopt their business models, and when they kept the same business model, dependent as it was so much on classified advertising, which kind of evaporated [with] the rise of Craigslist and other free services, funding journalism became a challenge in many markets, except where you had publishers who were able to find ways to scale their businesses and adapt.

And so you do see that with the national-oriented news publishers where the quality of journalism is as high as it's ever been, if not higher than ever. And they have fully national, if not sometimes, international, scale in their operation. But this means that when it comes to topics of national importance, journalism probably is as good as ever. When it comes to local matters, it probably has never been worse, and will only get worse as time progresses.

That's a challenge, because some information and means of communication are depending on regionally specific issues. It's definitely going to be true that those consumers who were dependent on their local news publishers, or their free ad-supported publishers, will find themselves lacking in the same depth of information that those who require or rely on national topics will find.

Fake news and active conventional disinformation campaigns, I think, is obviously a real problem and likely to get worse, if only because it's been demonstrated to work over decades and I think using social media platforms in recent years has proven very . So, I think that while it's true that there's more awareness among the platforms that this sort of thing exists, it's not clear yet that they've taken anywhere near enough action. And where they are taking action there are counter actions that can be taken. So, I think that the problem with fake news and disinformation is only going to increase as time progresses.

This overlaps with a bigger problem we have around distrust of news and information more generally. It's not helped by the fact that social media platforms have not done adequate jobs preventing the distribution of fake information. But then it's made worse when we have leaders who vilify reporting they don't like and news they don't like, causing a conflation of the terms that really undermines trust of the whole industry and the whole ecosystem, and all information getting distributed.

This could become a substantially greater problem, of course, when we do face real national crises where consumers, individuals may not know what to believe, who to trust. And unfortunately, that can cause all sorts of negative consequences for society at large.

Looking to the future, deepfakes are probably the one thing that is starting to come up a lot, and we can imagine how that could play out. It really feels like an amplification of the problems described previously. But certainly making something visual makes something more resonant with consumers, and so I think the idea of the deep fake is a way to visualize that fake news or fake ideas, is certainly more problematic also a continuation of the same problem.

Now, I think it's worth talking about the solutions that could mitigate some of these problems. The first thing is that social media platforms could end up imposing more stringent know-your-customer rules to make it harder for either paid advertisers -- often agents of disinformation

-- or consumers to place content on their platforms. These are generally private platforms who historically have been free of any obligation to restrict information distribution.

We may see legal changes that cause them to have to care, but all else equal, the publishers -- social media platforms themselves -- may choose to be more stringent in how they allow individual providers' information to post that information. So that could play out. More generally, changes in policies around acceptable content distribution is another path forward that could help.

A bigger issue that's more of a societal solution, and I haven't seen a lot about this, is investing in media literacy would probably go a long way towards solving these problems. In much the same way as financial literacy is a thing, and certainly large numbers of consumers are savvier investors, are savvier participants in the economy, because they know some of the basics around how to make money, how to save money, how to avoid being swindled. The same can be done with respect to media and information.

And I think that iIt is increasingly important for consumers to understand how news is produced, what passes for quality news, what makes for sketchy news, how to independently verify news and information, how to go to source material to check what consumers are being told. These are all very doable things, and it's not unrealistic to think that some entity, governmental or otherwise, could take an active interest in increasing media literacy across society, certainly at the above the very low levels that we have today.

With that, I hope you have a good conference and thank you for listening. Again feel free to reach out. You can contact me at [redacted] with any comments or questions. Thanks very much.

Anonymous, Russian Warfare Expert, Future of IW (transcript), 7 Sep 2019

Good day. My name is [redacted] and today I've been asked to talk about a few Russian operations, namely information, cyber, and electronic warfare.

All of these topics are actually very relevant in an age that's beset by fake news, deep fakes, spoofing, mimicries, and a huge reliance on social media. For Russia, this is also a very important time because the country is host to a lot of very gifted code writers. They have some excellent mathematicians, and they're also a country right now for which truth is a moving target. And we are finding that we are in an age of fake news, they are having some success with their ability to manipulate media and mass consciousness.

I'd like to start the discussion by looking at a concept called "reflexive control." Reflexive control is defined as trying to get someone to do something for themselves that they're actually doing for you. In other words, if I can get you to agree to a concept for which I'm interested in furthering, that would be the end element of reflexive control.

Within the information age, Russia has found that out on a battlefield that they like to insert what's known as "information packets." These packets are prepared by a very special table of organization and equipment that studies the information-psychological capabilities of an adversary. So, for example, if they were going to confront Estonia or some other Baltic Nation, they would have done a study of what type of moral, psychological situation exists in those armies, and then try to exploit any weaknesses they may have found with these information packets.

When Russia defines Information Warfare from a military point of view, they note that it has an information-technical and an information-psychological aspect to it, but also that an element of information warfare is to force a state to make decisions in the interests of the hostile party. So, in other words, reflexive control is embedded in the definition of information Warfare.

Within the cyber element, we find that something as simple as a phishing probe would could be considered clearly as a reflexive control operation, because what you're trying to do is to get someone to open an executable file for themselves when actually they are doing something for you, which is downloading a virus.

With regard to electronic warfare, reflexive control here is, just as an example, it might be offering a fake electronic warfare intercept to an opponent that indicates to that opponent that a force may be gathering and ready to conduct an offensive in a certain sector. That may force the opponent than to rush forces up to that sector, when in fact that was nothing more than a fake electronic intercept, but the end result is you got an opponent to do something for themself -- take care of that sector-- which you were really doing for yourself -- getting forces moved to one sector when actually your main attack might come through another.

A second area that would be worth exploring is the concept known as "disorganization." I think the concept is basically defined as, how do you deprive an adversary of his ability to organize and accomplish combat tasks? That would be a general description of disorganization. I was told years ago that a key element of information warfare in Russia is the ability to disorganize someone.

It's a word that we don't use often, if it all, in our Western lexicon of information warfare.

For Russia, within the information aspect, you might find terms like "information weapons," "information struggle," "information confrontation," "information strikes."

And there are a host of verbs that would indicate to you that this is an attempt to dis-organize an opponent: some might manipulate, destabilize, destroy, discredit, provoke. All of these items and methods are aimed at disorganizing an opponent.

Within the cyber element, we see that Russia has focused on what they consider to be weak space links that NATO has, and they want to do what they can to take advantage of these weak links in order to dis-organize that space force.

Russia has a concept also known as SODCID, strategic operations for the destruction of critical information targets, and that would be, certainly, a way to disorganize an opponent's infrastructure in case of their determination that it was time to enter what they call the initial period of war.

With regard to electronic warfare, we see a host of operations in the electronic sphere aimed at disorganizing an opponent. Each EW Brigade is now developing what they call a "disorganization plan" -- a way that they can dis-organize the command-and-control apparatus of an opponent that they're facing.

They are also modeling adversary C2, looking for weak links in that structure. And recently, the commander of the electronic warfare forces in Russia has noted that "very soon," he didn't say when, he just said "Soon," electronic warfare will decide the fate of all military operations. So there is quite a reliance, it seems, at this point in time, on the disorganization concept.

Finally, this ideal of Russia looking at truth as a moving target. We were quite surprised

as we looked back at how this concept has developed. We certainly noticed it in regard to the Malaysian airliner that was shot down. The West has come up with one developed scenario of what happened. That includes voice intercepts and photography of big systems that were in the area, and meanwhile, Russia has developed seven or eight different variants of how this catastrophe unfolded. So for them, it seems truth is a moving object that they can work with as they deem necessary.

Back in 2015, we found some of the most startling comments that really, perhaps, indicate that there was a strong motivation in that year to begin looking at truth in a different way. The Minister of Culture, Vladimir Medinsky, noted that history is open to not only interpretation but also mass propaganda. There was an article in Moscow Times that noted that "history plays tricks on those who think it is actually ended," which indicates obviously that history might be reconsidered at various intervals.

And there was an article in Military Thought, a Russian military journal, that noted two important things to me. One, it said that "information has now become the center of gravity for operations as much as power." And [two] there was a statement that said, "the mass consciousness can be manipulated through the media, much like a psychoanalyst injects an idea into a patient's head."

So with this idea of moving truth, the fact that it's not fixed, that history says it's open to interpretation at various intervals, we are seeing, it seems, quite a different set of responses to any incident: there's nothing fixed, it's open to further interpretation as the Russian see fit.

With regard to the cyber element, I think that the most significant development there, has been deep fakes, in that a video now can be altered to such an extent that it's hard to tell, really, if that video was real or if it was altered. Deepfakes are going to be in area of real concern, I think, for a lot of governments.

I really thought that Danielle Citron, professor at Maryland, perhaps said it best that if there's a video out there that someone doesn't like about them, they can merely say that "no, no, that wasn't me; that was a fake' that someone has altered it." And she ascribed to that concept, the idea of a "liar's dividend." The liar can pass off what they really said onto the fact that it could have been a fake video.

And finally in the electronic warfare side, of course, we see spoofing now. The Russians have used it to, in some instances, hide the location of key facilities or to mask the movements of President Putin.

So, in summary, we have deception, and we have truth as a moving object, and we have the ideas of disorganization to cover all three areas of these operations, of information, cyber, and electronic warfare.

I would add one more comment before closing, and that is, every year in April, the Russians have hosted a conference in Garmisch, Germany. In 2011, the US delegation asked a member of the Federal Security Service of Russia to rank-order the cyber issues that most concern them. And the top two were: escalation models that get out of control -- that was number one -- and number two, was any attack on critical infrastructure. The thing that seemed to bother Russia the least, in that list of 10, was industrial espionage, perhaps because they were doing so well at it. But I think it's important to note that there is a concern over there on things getting out of control in the information, cyber, and electronic warfare age.

I thank you for your attention and I hope you

have a great day. Thank you.

Cole, Future of IW (transcript), 9 Sep 2019

Hi, I'm August Cole, the author of Ghost Fleet; a non-resident senior fellow at the Atlantic Council; I work on creative foresight at SparkCognition, which is an artificial intelligence company; and I consult with various entities on foresight and narrative futures.

That said, what I'm about to speak about for the next 5 minutes or so reflect my own opinions and ideas not any of those organizations.

It's an honor to speak to the Threatcasting lab cohort and I wish you luck with this engagement.

I'm going to run through five or six things that I think are really intriguing, both from a creative point of view, but also from an analytical perspective in understanding the information on the environment in the next decade or so, really kind of pushing almost into the 2030s.

It's really fertile terrain to plow for the kinds of stories, characters that I think walk forward many of the truths and trends that we see today, but in often more dystopian, and sometimes optimistic ways, we can create a pretty realistic picture of possible futures.

I don't think it's possible to create a perfect rendering of the exact future we're going to have, but that's the sort of challenge I think that those of us who like to imagine all sorts of things are constantly striving to avoid.

I'm not looking to create a checklist of the actual environment, you know, 10 to 15 years out, but rather to get some tools today, in 2019, to understand some of the possibilities that might be out there.

Besides what fun would it be to actually know what was really coming down the pike?

The first thing I was going to talk about was the fragmentation of our personal realities.

You know, you can see the airpods I have plugged into my ears, the phone that you can't see that I'm recording on, all contribute to an increasingly impersonalized electronic relationship with, you know, consciousness, collective, and individual.

And that has profound implications, of course, in politics, as you've already seen, but it's going to start impacting the battlefield, particularly more both in the kinetic space but also, of course, in the information domain.

What I have been exploring through some of the short stories I've been working on is the ability to shape and wield different realities to create tactical advantage.

If you're in an urban environment, which is has been recognized as a generally very difficult challenge for western militaries to navigate, thinking about the ways that the movement of forces, for example, can be camouflage or concealed or broadcasted through connecting with inhabitants' augmented reality and virtual reality spaces.

The ability to make a tank look like a garbage truck, is one construct of that; to make a rebel fighting group look like an ally or vice versa, I think expresses the kinds of AI-driven environment bending and shaping that we're going to start to see.

Essentially, if you can imagine it, you'll be able to do it in a way that confirms, again, tactical, and of course, strategic advantage.

The other aspect of this relates to how did this get done.

I think China's integrated, again, algorithmically-driven, whether it's the

social constructs that are being engineered towards stability and prosperity at home, are going to start finding their implementation in countries that are that are buying into the physical infrastructure through One Belt, One Road, or belt-and-road initiative projects, you know.

If there is a Beijing consensus on privacy, on data, on the economics behind all that, working in a state-forward approach, that too, is going to have a very interesting effect on the kind of conduits that the individual has access to when it comes to augmented/ virtual reality.

I think we're getting closer and closer to seeing what that will look like; if you can imagine, for example, what the Beijing Olympics would look like in the mid- to late-2020s, you could quite realistically have a very different experience than what we saw last time around, in part, because the way that people who are experiencing that from abroad watching it would be seeing a very personalized interpretation of that.

That would, I think, be a reflection of the kinds of machine learning cutting-edge technology coming out of China and environmental, you know, artistry, if you will, so that you don't need necessarily turn off all the factories in the suburbs of Beijing to clear the air -- you can just air-brush it out, if you will, and control the social media feeds of the athletes hacking and coughing and complaining about that.

The other aspect of the operating environment, too, and I think this is especially interesting, because a lot of the interest that I've had in the past about setting the privatization of force and privatization of national security, is focused on hard security.

But we know through the information domain breakthroughs that companies like Cambridge Analytica show this having an effect on U.S. political process and other countries, that there is a whole other side to this kind of partnership between states, independent actors, and private entities in political or corporate.

So in thinking about the kind of public-private forces matrix where mercenaries are working on behalf of oil companies -- that's an old model, 20th century.

The new model is something much more informatized and hybridized, where, you know, data becomes the kind of marching force, if you will, not necessarily having, you know, Hind helicopters like former British or South Africans executives once did.

You know, the information domain can allow you to rent proxies, you know, for very short periods of time to create effects that are really important militarily, and that's something that western forces and governments are going to have to start understanding: where are the boundaries and rules, and when those sorts of rules might get broken for operational advantage.

You know, the idea of data access, and kind of almost like an ethical arbitrage, is something that I think you're going to see more of particularly in [the] Special Operations Community -- targeting is going to be really difficult in denied environments.

The idea of a small teams needing to locate individuals without perhaps the conventional sensors that are kept at standoff range, because of, like, ground-to-air missiles or other defensive systems, really pose interesting questions about how do you find someone again in a dense urban environment and other kinds of terrain that that would otherwise be pulling a proverbial needle-in-a-haystack?

Commercial data, whether it's wearables, you know, the IOT proliferation and everything from like, you know, our socks and shoes, to the glasses were going to

wear, we're going to be spinning off data through IP addresses for each of those devices.

That's going to be targetable and useful for targeting and I think that's going to lead to a kind of new standards and norms that will be broken from time to time, much in the same way that we're, kind of reconsidering what laws of armed conflict and even just war ethic, you know, means in the information era.

And this also, I think, ties into another aspect of this, too, which is: How do we trust what we see and what we know? How do we trust the forces that are deploying in a country's name? For those forces, how do they trust the people and machines alongside them?

And I am really intrigued by this question because the speed of some conflicts will be so fast that when many of these systems are being used for the first time, whether it's a loyal wingman, whether it is an information algorithm -- we may see those conflicts and engagements end faster than the trust cycle can be established.

So, in many ways, the force, or the side, if you will, that is able to experiment and develop those kinds of patterns and relationships with technology are going to be at an advantage because they will establish that trust cycle and be able to use those capabilities more efficiently.

And that speaks to more training, and experimentation, but also to doing so within a bounded and hopefully ethical way.

You know, the last thing I would close with: one of the great ways to get to come up with stories is to start thinking about the unanswered questions and relating them to the conundrums of today.

You know, one of the things I've been considering is when we consider, when we think about, some of the banned weapons today, like cluster munitions, which still have, according to many militaries, intense relevance, you know, for stopping Mass Attack; I'd say a North Korean Advance on South Korea; And the US has not agreed to stop using such systems.

Like, what is the information domain equivalent of such a capability or weapon and where will the legal norms fall short, where will they be applied, and which countries will abide by them?

You know, the Campaign to ban Killer Robots is focused, of course, on the kinetic, but I think it totally misses the conversation, which is more urgent, perhaps, on the information domain.

And I think that's one example of many that point to these kinds of questions that should be explored.

So I'll sign off here from, again, Marblehead, Massachusetts; this is my home office.

It's August Cole from the Atlantic Council, and I wish you all good luck with your conversation.

Coon, Future of IW (transcript), 9 Sep 2019

I am Cyndi Coon, the chief of staff at the Threatcasting Lab at Arizona State University.

I recently curated a Threatcasting lab workshop around weaponizing narratives.

This happened because the community really put out a call requesting coming together as individuals around disinformation, misinformation, and malinformation.

We conducted that curated workshop and the Lab produced a report of the findings.

This report, now known as information

disorder machines, or IDMs, had key findings as a part of the outcomes.

Those findings really included the following: in the coming decades, advances in technology like artificial intelligence, machine learning, quantum computing, the Internet of Things, smart cities, autonomous vehicles in air, space, and land will enable adversaries of the United States to mechanize information disorder to influence, manipulate, and harm organizations and individuals.

These coming information disorder machines will be targeted broadly at groups and geographies.

AI and ML will allow for increased, if not complete, automation allowing IDMs to adapt in real-time down to the individual level, creating personalized attacks, while operating on a mass scale.

The emerging threats of IDM's lie in the unique pairing of their real time micro-targeting and the macro effects that they can have at scale.

This is a direct threat to the National and global Security as well as threats to the United States of America.

Some of the threat futures that were identified include: adversaries using IDMs to incite violence and tribalism; encouraging anti-federalism; inspiring populations regardless of political affiliation to question the authority and the relevance of the United States government and the Union.

This destabilization will distract populations, governments, and militaries focusing on inflamed issues so that other adversaries can gain advantages elsewhere.

Generally, adversaries will exploit desperate conditions or catastrophic events to sow unrest and inspire mistrust in traditional organizations and governments, ultimately encouraging individuals to move to violence.

Corporations will use IDMs to increase profit, reach, and competitive edge while causing harm to individuals and each other.

Citizens, and special interest groups, non-traditional adversaries, will use IDMs to weaken the union of the United States, the education system, and the strength and resiliency of society.

Lin, Future of IW (transcript), 10 Sep 2019

Cyber enabled information warfare is not cyber war. This distinction is in distinction that has been missed in large parts of the public debate. In the wake of the 2016 presidential election, many commentators ranging from Dick Cheney to Hillary Clinton asserted that Russian interference in the US election was an act of cyber war, or cyber Armageddon, or cyber 9/11, or a cyber act of war. These comparisons are wrong or at least they're misleading.

Cyber war and conflict targets information and computers in cyberspace and adversary is pursue cyber war by taking advantage of the flaws in information technology of design, of info of implementation. By contrast, cyber enabled information operations, information warfare operations target human minds. That's what they go after, the human mind, the vulnerabilities in the human mind, and they prosecute information warfare operations by taking advantage of the technical virtues of information technology.

Consider that Russia exploited the social media platforms exactly the way they were intended to be used. They, for example, directed selected advertisements and other content to very narrowly defined audiences. They exploited automated accounts to amplify selected messages. They took advantage of the porosity of national

borders to information flows to transmit content internationally. They took advantage of the very algorithms that the social media platforms use to increase user engagement with advertiser and user generated content.

Now what are cyber enabled information warfare operations about? Let's start with informational warfare operations per se. The broad goal of such operations is to shape the target audiences, views, attitudes and behavioral predispositions with respect to other people, institutions, nations, and the like.

One typology that I find helpful is to think about information operations, information warfare operations is propaganda operations, which are what you usually think about as, as propaganda, false or more often a true false mix to audiences to influence their opinions, attitudes, emotions, and the like.

Another type of operation is what I call chaos producing operations. These are messages that are sent simply to confuse and raise the level of noise. For example, trolls producing fake disaster messages without any obvious purpose. They don't have to be consistent. They just have to frighten some people. This sort of operation is, is throwing something up against the wall and see what sticks.

And a third kind could be considered hack-and-leak operation. The hacking part is part of cyber war. This is when you compromise a, an email account, for example, to get out secret information or information that the email user would rather keep secret, but then you publicize it all over the place and you spread it around on the theory that if, if it was secret, it must therefore be worthy of attention. And this takes advantage of notoriety and so on. That part doesn't, isn't a part of a cyber war. But it is a very much an important part of information warfare operations.

Information operations have many purposes. They can inform, which is a good thing, but they can also distract people from the right things to be looking at. They can overwhelm a target's attention. They can confuse and disorient. They can mislead, they can provoke and outrage and stimulate unthinking emotion. And, and, and the like.

Now information warfare operations take advantage of vulnerabilities in what you might call the human cognitive architecture. And it's now by now well known that human beings use have two different ways of thinking about the world. One is what you might call the intuitive heuristic fast thinking. The other is a much more deliberate, analytical, reflective, slow thinking based on logic and, and, and the life and the success of information operations largely depends on the exploitation of these of the difference between the two. Trying to [fourth] take advantage of intuitive and heuristic and non-analytical thought to to do there to, to achieve their effects. Hitler of course, was a master at this of stimulating emotion in people and in getting them to only think about what he wanted them to think about and, and so on.

Then the question is, what does cyber bring to the table for the information warrior, for the information operations warrior? Imagine what Hitler could have done with the internet and social media. What modern technology brings, cyber technology brings, is high connectivity, low latency, anonymity, anonymous production of sorry, inexpensive production of of information. Democratized access to publishing capabilities; it eliminates intermediaries so that people can get their own information, which means journalistic controls are no longer in place and, and so on. And the taking advantage and taking advantage of these characteristics of information technology simplifies the, the job of the information warrior quite a bit ;because now what they

can do is they, they give large megaphones to what formerly were fringe players. It's easier to create filter bubbles where people can consume only information that they're comfortable with.

The anonymity of the internet means that there's a lack of accountability. Now it becomes possible to target very narrow audiences and, and, and the like. In the future, we'll see other IO attacks of concern: forged emails; forged videos, which you've seen; forged audios; highly selective targeting built on of messages going to people based on their stolen Equifax profiles, in addition to their social media profiles; perhaps conversational chatbots that are artificially intelligent that can actually engage people in a more extremist producing, radicalizing dialogues targeting individuals during times of emotional vulnerability to increase their receptivity to to, to messaging.

The problem in all of this is that what the information warrior has done is to take our strengths against us, turn our strengths against us. The first amendment is there to protect free expression of individuals. And now what we have is an environment in which lots and lots of people are shouting in a very chaotic way and there is very little ability to differentiate between stuff that is actually useful and advances the public discourse from stuff that just inflames emotion and just gets people mad at each other. And that's the problem that we face.

Reed, Future of IW (summary of transcript), 9 Sep 2019

I remember very clearly, November 2012. I was sitting in an office thinking about what we had just done. I was CTO for the Obama campaign. We just won this election. We'd done it heavily with data, heavily with technology. We'd done it because we were able to do it because our wonderful volunteers had given us access to their data via Facebook, via email, via grassroots organizing; all of these things had happened and it worked out really, really well. I remember thinking, "This is incredible! What an incredible, incredible world!"

Well, fast forward eight years. A lot has changed. Our narrative around data, specifically within elections has changed drastically. But what hasn't changed is the amount of microtargeting, the amount of data that we are exhausting from our bodies. This data exhaust, or as I like to call the social exhaust -- the data coming from phones, from computers like the one I'm recording this on.

All of this data is sitting here just pushing out. We are being targeted by corporations, by nonprofits, by NGOs, by everyone. Every single person is, I don't say a "victim" of targeting, but in 2019 and in 2020, targeting it is our everyday. From the mail we receive, the paper mail -- this anarchistic form -- to the banner ads we receive, to the spam calls. We are being targeted because of our data.

Well the amount of data we have exhausted from our bodies, from our behaviors, from our patterns, has doubled, tripled, maybe quan...some huge number, in the last 8 years. Well, I think in the future it's going to just get worse, or maybe better. I'm not certain I have a strong judgment on it, but what I do know is as we pair this data with machine learning, with all of these advanced, exciting new technologies that are coming out right now, things are going to get very interesting.

AI and machine learning allows us to mechanize a lot of this targeting; we've seen that over the last 10 years. I think what we need to see is that as we give out more and more data, does AI and machine learning start to weaponize this technology? Does

micro-targeting become an adversary that we as humans cannot survive against? Or is it an adversary that we are collaborative with?

I'm not sure, but I think a lot about, if I was doing this work, the work that I did in 2012 and 2020 and 2024, etcetera, how would I do things differently? And I think the question is, what do we do about this data? A lot of people don't even know -- that's why "exhaust" is such a good word; they're not aware that they're pushing out all this data. A lot of people are aware -- they choose to take actions to stop it, to minimize it, but even then, there's so much latent data that we're out-putting that it's very difficult to control. And so, from a targeting perspective, we are always, always a target.

APPENDIX D

RAW DATA

Research Synthesis Workbooks

(Second Workshop)

	GROUP 1			
Data Point #	Summary of the Data Point	Implication	Why is the implication Positive or Negative?	What should we do?
1	Tribalism becomes focus of IW operations	expression will have crazier and wilder ways of being expressed; tech will enable this; what you can say on social media is not what you can say in person;	this will have a real implication of who gets to say what and this will narrow; voice capital; those who will get to say what they want and the rest who have to ration it	
2	Speech Modulation/Regulation	Counter to free speech demands; but provides coherent, consistent narrative	terms and conditions have more power to regulate speech than the courts	
3	reflexive control	All it takes is the right set of seeds to make people move in a direction you want and then it grows by itself...it doesn't necessarily need additional care	Can be economy of force in resource constrained or highly-scrutinized military operations	
4	disorganization, & chaos producing operations	Reduction in resilience of society; also: consider the analogy of "wrestling" - you can win in wrestling without a pin; distraction and causing chaos becomes an operational aim all by itself	Breaks long-standing threads and values that built society in the first place; continually keep argument inflamed —> prevents getting at solutions	
5	filter bubbles	People reinforce favorable ideas and don't get to see other perspectives;	reinforces boundaries and barriers; prevents empathy bridges	
6	human cognitive architecture	reactive vs rational decision making systems	Not pos/neg - this can be exploited for good or evil	
7	individual targeting	operations targeted towards atomized individuals vs members with affective/moral ties to society	breaks social ties; can create new ties not locally anchored	
8	AI chatbots for radicalizing dialogue	Radicalization may occur without (much) human intervention	May be able to monitor AI chatbots with other AI	
9	real time micro targeting w/ macro effects	New ideas can be generated faster than we can respond to them; personalized content that really resonates with you		
10	movement to violence	this is assumed to be bad/universal		
11	Shared conceptions of reality	mass consciousness manipulated through the media; truth as moving target; meaning of history		
12	liars dividend	liars can deny the deep fakes; how will this affect legal system	what's the impact on society/institutions & legal frameworks	
13	information as center of gravity	center of gravity is an adversaries ability to wage war		
14	escalation models	what keeps things from getting out of control? what drives things out of control?	Nationalism problem - if fire gets too big, your own house burns down	
15	attacks on critical infastructure	if something breaks, it takes a long time for things to get fixed		
29	Narratives can be weaponized to divide the population/USA	whole of society issue: Citizens could be used to weaken education and society, democracy has always required a well educated population	Positive and Negative	Encourage cross-sector learning of best/worst practices (Academia, public, private sectors) hiring, education and professional development practices.
17	Micro-targeting at Macro-scale: IDMs adapt at the individual level, at a mass scale, unique paring, rel time micro-targeting, to have macro effects could have a negative impact on the world and the USA.	whole of society issue: Citizens could be used to weaken education and society, democracy has always required a well educated population	Mostly negative	Build bridges between "Right coast/Federal govt centric" and "Left coast/siliicon valley centric" communities/cultures. Fed agencies reach out to tech firms.
18	Tech tsunami: AI, 5G, AR/VR, autonomous vehicles, IOT, UAV, etc can be used to "mechanize" disinformation can be used for harm, machines will be targeted at groups and geographies	Increased threat/attack surfaces with little or no human implication in the unmanned vehicles. Creates increased spectrum of security threats (both physical and biological)	Continue to adapt/learn the new technologies both offensively and defensively. Embrace/experiment with new technologies to help identify future threats (i.e. adversarial Machine Learning). Integrate Silcon Valley with key military agencies to more quickly embrace the new technologies.	Incentivize cultures of embracing new technologies, societal comfort w/ embracing and experimenting with new technologies to help identify future threats and tactics. Can't have seams between offensive / defensive operations! Create global policies and laws regulating AI, IOT, 5G, Autonomous Vehicles.
19	Chaos producing fake messages that will fool general population			
20	Hack and leak operations compromise secret or personal information. To create attention to that information.			
	Information operations can inform, distract, confuse, create fear. The human cognitive rectitude,			
	The minister of culture and information in Russsia indicated that history is movable, and can be reconsidered or manipulated.			
	The most significant Developments is deep fakes because of the quality of the fakes. If there is a video, the liar can pass off as a fake any video they do not like			
	Spoofing can mask movement of VIPs or hide military installations			
	Disinformation: Information that is false and deliberately created to harm a person, social group, organisation or country Misinformation: Information that is false but not created with the intention of causing harm Mal-information: Information that is based on reality, used to inflict harm on a person, social group, organisation or country.	It's important to distinguish messages that are true from those that are false, and messages that are created, produced or distributed by "agents" who intend to do harm from those that are not.		
	how does social media work	russians were able to see the capabilities of the social media systems	If Russia can do it, why can't every other adversary do the same thing?	
	Mind/Tech Interaction	3 info ops: chaos, propaganda, hack & leak ; we've taken away all the brakes between social interaction (flawed assumption that connecting people is "good")		
	misinformation vs malinformation vs disinformation	are these separate types of attacks		
	Points IDMs will adapt at the individual level, at a mass scale, unique paring, rel time micro-targeting, to have macro effects.		attack surface	
	Selected advertisements, international information flows, took advantage of the algorithms, the broad goal is to shape the audience and prepare them for suggestions			

	Intuition and nonanalytical thought can be taken advantage of			
	Reflexive control, trying to get someone to agree to a concept that you are interested in			
	Russian EW seeks to study the moral, psychological, and political things in that army. An element is to force a state to make decisions that benefit the hostile state.			
	Another area disorganization, depriving an adversary of his ability to complete combat tasks. Information weapons, struggle, strikes, and confrontation			
	Soon EW will decide the fate of all military operations			
	Informaton is now the COG. The media can manipulate the mass consciousness.			
	In the future, forged email, video, audio, targeting individuals with AI chat turn our elements like the 1st amendment against us.			

	GROUP 2			
Data Point #	Summary of the Data Point	Implication	Why is the implication Positive or Negative?	What should we do?
1	one-on-one marketing relationships	Brexit, individual messages that cannot be countered if never seen by those that could counter		all marketing must have a witness, abiltiy to reseach what was done and provide accountabilty
2	Weaponized marketing media	data privacy rights, getting paid for your data; memes		
3	solitary confinement of your media environment	leads to bubbles and extremism; moves in polarizing direction		
4	complicent in targeting	training from a young age to believe marketing		
5	connection of the fringes	no one has to feel alone on the internet. Communities for all crazies on the frige		
6	cyclical nature of ideas	Ideas don't die on the internet. Steer the discussion to recycled ideas. Healty debates get sidetracked		
7	virtual reality and information spread /immersive content	ability to create alternative worlds and creation of virtual friends and support/ unsupported communities		
8	Data exhaustion and how is it paired with ML and AI	AI can steer the targeting, the more data requires advanced analytic tools		
9	News desert: National news increased professional and decline of local news	degrades trust in local governement		
10	Volume of the money in fake news and marketing	how do you push against capitalism in a free socitey		
11	Deep fakes and information campaigns	video evidence cannot be considered reliable		
12	5G gives availability to push huge information	bigger tunnel for information and disinformation		
13	Social media not curating or updating information space	no labeling of fake news; no cleaning of things that have been shown to be false		
14	Leaders decribing divergent views as fake news	need for moral leadership for the free world. Leaders can be complicent in the degredation along with media		leadership code of ethics
15	In crisis: no idea where to get their true news	Death of trusted printed publishers		Meida literacy campaign
16	Concerned of manipulation of mass reactions using marketing techniques, threat of coercion by company	Customization/personalization, private/highly private, highly adaptive, greater fragmentation of personalized content and info	When we do it it's good/when someone else does it, its bad; direct political implications - not onoculated to critical thinking	Governance; Education of citizens; chaos
17	Generation born into curated, personalized content have no resistance, resilience or immunity	Will not have prior stated in terms of innoculation; don't know what could be different as reality as opposed to pre-Internet generations	Have already been indoctrinated into 24/7 info and curated content as reality/the norm	Education of young people in schools for critical thinking, media literacy, data/tech/privacy literacy
18	Science says frontal cortex not fully formed in males til 25 - how are males under 25 more of a target from 1st data point	Less immunity to affects; easier to radicalize for young men such as Muslim refugees		Education from their own
	Social Media effect on Societies: open vs closed societies	possible for authoritaions to supress, but opportunity to share U.S. Views		
	Marketing focus on friction: Nike	tension and fear in the public being used to drive markets		
	can't self regulate crazy			
	Deception is built into marketing	marketing is viewed as trusted source but yet we know they have a purpose to create the information		
	Marketing for propaganda use	The dark arts of marketing	Eye of user and philosophy	
	"We assume people less smart than us are the only ones affected. "	The elite (education socio, race) know better than the masses; can't be fooled	Blindspots	Emotional Intelligence vs. Artificial Intelligence

	GROUP 3			
Data Point #	Summary of the Data Point	Implication	Why is the implication Positive or Negative?	What should we do?
1	200 years of Democratic institutions being attacked	Cambridge Analytica is a direct attack on democratic institutions; how do we identify the enemy? Breakdown of country into regional de-stabilizing conflicts being encouraged by a lack of governance. Plays on traditional senses of trust in traditional institutions. Attack on soldiers, systems, and institutions. Two-front war analogy... only coming from multiple fronts. Parallels with the media literacy	Negative	Data literacy; Shared cultural narrative; Education (what it means to be a citizen)
2	Serious gap in Data literacy	narrative targeting; spreading of dis, mis, and malinformation	Negative	Educationl; in advertising it becomes a matter of self-interest
3	Military advantage evaporates in 2030; boundaries; dissolution of boundaries	Many more skirmishes because the assymetry is greater; taking Crimea without firing a shot; Cost of war goes to zero and physical cost goes zero	Negative	New interconnected norms (treatise); Increase the cost of violating boundary-less behaviors
4	Us against Us; our democratic ideals being used against us	Elections; polarization; chaos; social and political violence	Negative	Consequences; laws
5	Manipulation in augmented reality	Making a tank look like a trash can	negative	technology;
6	Responsible and ethical use of AI. As human enhancement via AI continues to grow - we unlock the human genome and figure out how to enhance the human senses .. we will put stress on military policy and ethics that guide the use of AI. We will more be asking whether we "should" do something vice "can" we do something.	consequences wont be fully internalized, realized, and/or accounted for until it is too late. Also, if we are first to market - does not mean others will follow us. Are we putting ourselves/country at a disadvanatge if we don't go there. Is it even possible to draw a line in the sand that everyone would adhere to (when push came to shove).	negative (99% chance, 1% chance an ethical framework is powerful to regulate / deescalate abuse)	
7	What will be the standards for AI in a "just war" sense - we banned cluster weapons, but what about other technologies? We will inevitably overstep boundaries, how do decide which tech to use and why? What is out of bounds for finding someone or tracking them down via IoT?	how do we define bounds within the geneva convention sense especially if we are not the moral leader of the world; completely uncharted territory; we have adversaries that are racing to the bottom; much easier to set red lines in kinetic world (like banning chemical weapons or land mines) as these haev a visoral effect - how do we describe and then get consensis in the world on what is wrong	negative	
8	Managing data in a fully connected state. AI is very different from other technology used on the battlefield. Now, we are not just focused on the fight between militaries but really fighting data vs data OR algorithms versus algorithms. This happens in fully connected, converged state.	quality and quantity of data (in this state) to make decisions in real-time on actions is too much for humans, so need trusted ML/AI to do it. therefore, battles waged between who has the faster, cleaner tech to poison the other side's data collection and protect ours. how do we trust the data and algorithms? data integrity becomes essential in a fully connected world. Therefore, increasing the attack surface area.	could be either	
9	Closing income, education, and inequality gaps is the only way we can insure competitiveness and full participation in IW	there is not enough economic/education opportunities to make sure that everyone is participating, we have this opportunity to have better troops on the front line of info warfare; this is a whole of society problem to fix as the battlefield has moved out of its current definition and includes society at large; what happens if we can't develop a common understanding of the tech space (info space) for all of society? what if our adversaries conduct activities to ensure we can't close the gaps (as a long-term strategy to their dominance over us); what if our adversaiers are more focused on not just creating friction in society on a specific issue but really about deepening inequality gaps	negative	
10	Issues of free speech are no longer just the providence of individuals or governments. Corporations have a vested interest in this issue and can influence where societies head. (example Facebook)	corporations - with corporate motives or "for-profit" motives could drive decisions on what is free speech and how to protect it. Issues of public interest become mediated by private companies/contracts.	positive - we want businesses to be allowed the power to moderate the content that is published. negative - if that is the only way that we participate in public discourse (which is mediated by private industry) then what value are the constitutional ammendments	
11	Fragmentation of our personal realities where we have personalized relationships with our tech devices. Namely, to think about the ability to shape and wield different realities to create a tactical advantage. Example: camofalguing, concealing, and or broadcasting troop movements in urban terrain. (make a tank look like a garbage truck). If you can image it, then you can impose your ideas on others' views of the environment. another example is china photoshopping out factories and smog from teh next olympics	confusing people with fragmentated realities ... confuse about the truth so that you can deny everything. If everyone has different truths, what is reality?	positive - can see information tailored to you; also could help folks on the Autism scale to participate and understand the world around them if it is tailored to how they can intrepret life; negative - because someone is controlling truth	
12	The speed of an idea like social credit Netflix credit becoming reality in China.	sci-fi seeds ideas into the world in a way that places like China can pick up (authoritarian regime). should not stop though .. but it is a risk in sparking new ideas. Becoming aware of these new ideas helps us better prepare (tide rises for everyone).	positive	
13	What does privatization of information warfare look like past Cambridge Analytica? What do mercanies look like in the info world? People that provide a service to the highest bidder regardless of any moral questions	service = data collection or data analysis or hyper-targetted campaigns; CA was a prototype for mercenaries within this space (showed viability of the business model); this is a new industry that will be formalized in the future; crossed traditional nation state lines; could be corporations fighting each other OR corporations fighting nation states	positive if you are an info mercenary	
14	We need to be prepared for fundamental attacks on the democratic processs via the information/digital domain. ((by definition: this would be attacks against 1) a political system for choosing and replacing the government through free and fair elections; 2) the active participation of the people, as citizens, in politics and civic life; 3) protection of the human rights of all citizens; 4) a rule of law, in which the laws and procedures apply equally to all citizens). Think about the weaknesses that are exposed through massive amounts of data about citizens / society that technology could exploit.	we have no resiliency in our current democratic processes as we assume no one will attack; when people lose faith in these - it is a showstopper; this used to be a red line that other nation states would not cross; this is a human American spirit problem - why do people not take this seriously right now	negative	
	The immune system reaction to Russian disinformation has begun – there's the immediate response, and then the long term implications	immune systems in biology solve the problem differently. the body comes up with a custom solution with each time it fights a disease. if you think of our society's reaction to this - the solution will be a combination of regulatory, market-based solutions, etc. So, we will see an initial reaction and then will develop anti-bodies for a long-term solution. Think about yellow journalism in our American History high school class. we need to think about what the long-term, custom solution might look like and how our adversaires will react.	slightly positive as we assume that it is not terminal and our immune system will learn to help mitigate this in teh future	
	Electronic relationships affecting the battlefied			
	Conflict resolved before a trust cycle can be established			
	How do we trust what we see and know in an information rich environment; overdependence on information			
	Throwing off data exhaust; paradox; good and bad			
	If every is fighting against everything in all places we need to have full participation			
	No existing playbook on privacy and the use data			

Threatcasting and Backcasting Workbooks

(Second Workshop)

Team Members:	**Red Pawn 1**		
Team Title:	**Red Dawn**		
Estimated Date of the Threat:	**2029**		
Data Points			
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)			
Grouping 1	Tribalism - expression will have crazier and wilder ways of being expressed; tech will enable this; what you can say on social media is not what you can say in person;	expression will have crazier and wilder ways of being expressed; tech will enable this; what you can say on social media is not what you can say in person;	this will have a real implication of who gets to say what and this will narrow; voice capital; those who will get to say what they want and the rest who have to ration it
Grouping 2	cyclical nature of ideasIdeas don't die on the internet. Steer the discussion to recycled ideas. Healty debates get sidetracked		
Grouping 3	Serious gap in Data literacy	narrative targeting; spreading of dis, mis, and malinformation	
Threat Actor or Adversary			
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):			
1) State Sponsored			
2) Proxy			
3) Extremist/Terrorist/Hacktivists/Patriots			
4) No Specific Actor/Environmental			
5) Business	Business as threat actor		
6) Organization (e.g. political party, special interest group, religious group, etc.)			
Put your Threat Actor or Adversary here:	Business		
PART ONE: Who is your Person?			
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.			
Who is your person and what is their broader community?	young mother, 1st nations community, rural community, Pad, artist - Bailey - born 2009		
Where do they live?	Paducah, KY - 3rd most prominent micropolitan// shipping transport - Walmart		
What is the threat?	Chinese multinational wants to interdict		
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Chinese multinational creatres social media narratives - recycled memes, old stories about shabby product, underpayment of workers - first native american, then other subgroups, including the head of logistics, use AI autogenerated communities of fake workers complaining. emails and messages are interdicted with a phishing attack disguised as a link to the AI genreated Audio/video deep fake "exposee" videos - to secure logisitcs/operations credentials - also bots targets workers and employees - her customer data handsets have unique explicit user profiles/shopper hisotry		
Who else in the person's life is involved?	friends, coworkers, tribal memebers and customers		
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	actors intent is grwoth and market share, looking to create a dependency on their network and services - short term goal in interdicting Walmart, long term goal is capturing logistics inventory/port operations - 23 companies in paducah. Walmart is short term, logistics is long term. State-controled store looking. goal is to lock down logistics infrastrcuture to prevent lockouts (government)		
What vulnerabilities does this expose?	walmarts defenses work at a corporate level; not an individual actor operating outside critical infrastructure - access through her team to user info/ then to logisitcs		
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)			
Questions (pick two) from the drop down selections			
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>			
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?			
What will this make your person do that they normally would not?			
What is different and/or the same as previous events or instantiations of the threat?			
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	polluted feed with recycled stories about shoddy product / the probelm is only paducah / deepfaked geofneced data turd		
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)			
What will the person have to do to access people, services, technology and information they need?			
What are the broader implications of a threat like this? What might a ripple effect look like?			

Question One	Answer your question in the yellow box		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>			
Question Two	Answer your question in the yellow box		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>			
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)			
Questions (pick two) from the drop down selections			
Question One	Answer your question in the yellow box		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>			
Question Two	Answer your question in the yellow box		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>			
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)			
Examine the combination of both the Experience Questions as well as the Enabling Questions.			
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.			
What are the Gates?			
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.			
1			
2			
3			
4			
5			
What are the Flags?			
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?			
1			
2			
3			
4			
5			
Milestones:			
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?			
1			
2			
3			
4			
5			
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?			
1			
2			
3			
4			
5			

Team Members:	**Orange Pawn 1**
Team Title:	**The Best Team**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	Micro-targeting at Macro-scale: IDMs adapt at the individual level, at a mass scale, unique paring, rel time micro-targeting, to have macro effects could have a negative impact on the world and the USA.
Grouping 2	Death of trusted printed publishers
Grouping 3	Us against Us; our democratic ideals being used against us
Threat Actor or Adversary	
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):	
1) State Sponsored	
2) Proxy	
3) Extremist/Terrorist/Hacktivists/Patriots	
4) No Specific Actor/Environmental	
5) Business	
6) Organization (e.g. political party, special interest group, religious group, etc.)	
Put your Threat Actor or Adversary here:	3) Extremist/Terrorist/Hacktivists/Patriots
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Joe Snuffy - social media influencer at a univeristy
Where do they live?	Low econmic community in the suburbs of st. louis
What is the threat?	Deep Faked podcasts using his voice, similar enough to his topics the make it impossible to deny
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	People are questioning his new views, peers disassoiate, univiersity questions motives. Starts panicing
Who else in the person's life is involved?	close family, significant others
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	they want to use the legitamacy of the podcast to disseminate their message
What vulnerabilities does this expose?	truth verification
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	

Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	
2	
3	
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	
2	
3	
4	
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	
4	
5	

What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	
4	
5	

Team Members:	
Team Title:	**Dawn of the Rising Sun**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	attacks on critical infastructure
Grouping 2	Generation born into curated, personalized content have no resistance, resilience or immunity
Grouping 3	No existing playbook on privacy and the use data (esp. international agreements!)
Threat Actor or Adversary	
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):	
1) State Sponsored	
2) Proxy	
3) Extremist/Terrorist/Hacktivists/Patriots	
4) No Specific Actor/Environmental	
5) Business	
6) Organization (e.g. political party, special interest group, religious group, etc.)	
Put your Threat Actor or Adversary here:	State Sponsored
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Akito Naruhito, decendent of emperor Naruhito
Where do they live?	Japan
What is the threat?	Climate change is influencing Japanese strategic decisions to consider new territory to enable national/cultural surivival; Akito is a target of Chinese IW trying to divide her (as an influential political and military symbol) away from achieving Japan's "first boots on land" strategy in China
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Akito is the daughter of the throne reestablishing the Empire and dominance of Japanese culture through the pacific. She's responsible for establishing the resurgent warrior culture in Japanese culture
Who else in the person's life is involved?	Akito's daughter is 7, and has grown up in a hyper-connected world and is POINT OF vulnerability for digital exploitation. Compromising deep fakes of her daughter in sex has caused Akito to rethink the Japanese strategy to retake population/territory. She is now focused on finding the perpetrators who are attacking her daughter/ family honor.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Japan is mobilizing their community to regain their regional dominance that they had prior to WWII. They are looking for new territory to preserve the cultural /genetic empire. Women's duties to be mothers and warrior for Japan. As the daughter of the Emperor, she is the vessel for the hopes of resurgent Japan
What vulnerabilities does this expose?	Shame caused by inability to find the people who made deep fakes of her daughter

PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
What will this make your person do that they normally would not?	Value saving her daughter's reputation tied to her duty to country - unless she can nest the two together and the decisive military action against the perpetrators of deep fakes
Question Two	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	Sparks a very aggressive Japanese strategy to re-take Chinese land areas in opposition to previously arranged political agreements. This causes internal conflict between military and political powers within Japan. Logistics question regarding destroying the perpetrators.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	Deep fake, and automated deep fake generation; I don't need to wait to develop a deep fake compromising YOU, because China already did it and it's on the shelf; automated distribution capabilities without attribution to China
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	

Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	
2	
3	
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	
2	
3	
4	
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	
4	
5	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	
4	
5	

Team Members:	**Teal Pawn 1**	
Team Title:	**Artifical Democracy**	
Estimated Date of the Threat:	**2029**	
Data Points		
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)		
Grouping 1	Points IDMs will adapt at the individual level, at a mass scale, unique paring, rel time micro-targeting, to have macro effects.	#22
Grouping 2	Concerned of manipulation of mass reactions using marketing techniques, threat of coercion by company	#21
Grouping 3	200 years of Democratic institutions being attacked	#1
		not used to core of democracy being the target
Threat Actor or Adversary		
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):		
1) State Sponsored		
2) Proxy		
3) Extremist/Terrorist/Hacktivists/Patriots		
4) No Specific Actor/Environmental		
5) Business		
6) Organization (e.g. political party, special interest group, religious group, etc.)		
Put your Threat Actor or Adversary here:	organization: anti-democratic political party in USA	
PART ONE: Who is your Person?		
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.		
Who is your person and what is their broader community?	Middle School Civics teacher; Mrs. Foley; older gal that remembers how democracy used to work in the early 2000s	
Where do they live?	Iowa; Refugee camp as there is only 1 farmer left in the area;	
What is the threat?	Mrs Foley gets targeted to purchase textbooks that are re-writing history as anti-democratic party is changing society; influenced to burn old textbooks that might "correctly" describe history; in the future everyone's textbooks are personalized and open to the highest bidder for content - so, in real time - changing content exists ... all of which makes it hard for her to consistently teach; additionally, grading is out of her control as AI grades assignments; also, deep fake videos to change history (like George Washington says) real-time as people bid	
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	the anti-democratic party is starting to take power within the USA; influencing students of her; farm substidy is about to be voted out (which is influencing her community at large); voting is not working and folks in the urban areas have greater say in government than in rural areas (hence why the farm substidy bill is about to be revoked without understanding the impact on the nation); the internet took away her ability to parent Alan and influence his life choices ... therefore, she is feeling the changes in this environment both as a parent and as a teacher of children	
Who else in the person's life is involved?	(Alan) Mrs. Foley's kid in his 20s that is being groomed to be an alt-right terrorist;	
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	what the anti-democratci party wants to achieve: stop voting and get rid of elections; discourage participation in democracy; AI-enable fascism (let a computer make the decisions - techno-crat with fully formed AI .. to make best decisions for society as most of society is not competitent enough); anti-democratic party is afraid that American values will take hold again and people will start to participate in government again; they are also afraid of luditism ... people become skeptical of the AI that they want to be in charge/ that they will shut off feeds	
What vulnerabilities does this expose?	people are susceptible to hyper-targetted partisan; pure human lazyness; people vote by pop-up ads	
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)		
Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?		
What will this make your person do that they normally would not?		
What is different and/or the same as previous events or instantiations of the threat?		
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?		
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)		

What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	mass school suicide ... where micro-targetting within the curriculum convinced students to do it because the world is so screwed up (ads that they read in their textbook) ... covert operation by anti-democratic party to create mass event that they are the only solution to; makes studens upset about democracy; Mrs Foley - has a reaction to this - unsure how to combat this problem within the school and larger society
Question Two	Answer your question in the yellow box
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	via textbook with multi-media, personalized messages that convinced the students that our current world order and truth was not worth living in; targetted vulnerable population (youngin's) - Mrs Foley struggles to figure out how to protect her students from their textbooks
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	wore down the current system (sped up the killing of the current democracy and parties); sowed discord amongst the population; national education system goes away and now it is all chartered and for-profit schools; increased call from society for personalized products; embraced mult-media, learning platforms
Question Two	Answer your question in the yellow box
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	hyper-privitized AI that subscription based that makes you smarter and gives you an advantage in life/society; teaching to the test; starts as subscription model and then adds ads that influence you; it is real-time bidding for organizations to influence it; convinces society that this is needed to close the equality gaps; ///
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	
2	
3	
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	
2	
3	
4	
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	

4		
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1		
2		
3		
4		
5		

Team Members:	**Purple Pawn 1**
Team Title:	**Project Purple**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	how does social media work
Grouping 2	Generation born into curated, personalized content have no resistance, resilience or immunity
Grouping 3	How do we trust what we see and know in an information rich environment; overdependence on information
Threat Actor or Adversary	
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):	
1) State Sponsored	
2) Proxy	
3) Extremist/Terrorist/Hacktivists/Patriots	
4) No Specific Actor/Environmental	No specific actor/environmental
5) Business	
6) Organization (e.g. political party, special interest group, religious group, etc.)	
Put your Threat Actor or Adversary here:	
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Corporations + Information tribes/ Haves Have nots due to infrastructure access
Where do they live?	Urban/suburban/virtual = first world of US; rural, poor access; reservation = third world of US
What is the threat?	Huge divide between tribes and urban vs. rural
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Experience life as a non-citizen, cannot participate in society (politically, economically, socially, knowledge) fully
Who else in the person's life is involved?	Information
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Want to achieve information dominance - they are the controllers and governance of all information for purpose of market dominance. Corporate nation side; corporatism
What vulnerabilities does this expose?	threatens exsitence of current liberal democracy
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	Haves: apps, social media, messaging, virtual worlds that incorporate social; mind melding technology; brain wave messaging; consequence
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	

Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?		
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?		
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?		
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?		
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?		
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question		
Question One	Answer your question in the yellow box	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
Question Two	Answer your question in the yellow box	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)		
Examine the combination of both the Experience Questions as well as the Enabling Questions.		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.		
1		
2		
3		
4		
5		
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1		
2		
3		
4		
5		
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1		
2		
3		
4		
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1		
2		
3		
4		
5		

Team Members:	**Black Pawn 1**
Team Title:	**Apocalypse Now**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	Another area disorganization, depriving an adversary of his ability to complete combat tasks. Information weapons, struggle, strikes, and confrontation
Grouping 2	Data exhaustion and how is it paired with ML and AI
Grouping 3	The immune system reaction to Russian disinformation has begun – there's the immediate response, and then the long term implications
Threat Actor or Adversary	
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):	
1) State Sponsored	
2) Proxy	
3) Extremist/Terrorist/Hacktivists/Patriots	
4) No Specific Actor/Environmental	
5) Business	
6) Organization (e.g. political party, special interest group, religious group, etc.)	
Put your Threat Actor or Adversary here:	State Sponsored - Chinese Adversary
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Kai Foo Lee CEO and evil mastermind
Where do they live?	No country of residence - lives everywhere and lives nowhere (currently residing in Four Seasons Suite in Hong Kong) along with his 44 well armed security detail and 500 data scientists.
What is the threat?	Cornered the majority of AI/ML technology; controls education systems and hiring practices of all technology companies worldwide through his algorthmtic approach to everything
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Kai Foo Lee's love of life was misdiagnosed due to a fault AI/ML algorthrym in the US Healthcare system and lost her life as well as her unborn twin boys.
Who else in the person's life is involved?	Several unknown mistresses and his daughter who is the heir apparent for his global empire. Her birth mother is a Uyghur and lives off the grid converting feces into electricity further perputrating the between rural and urban.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Cleansing of humanity and reestablish a new world order where the United States is no lower a super power.
What vulnerabilities does this expose?	US Citizens are unknowningly participating in Kai Foo Lee's technology and manipulation (physical and biological) - hence rewriting textbooks in Iowa and Walmart's logistics. It all ties back to the MASTER EVENT from Kai Foo Lee.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	

What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	
2	
3	
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	
2	
3	
4	
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	
4	
5	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	

1	
2	
3	
4	
5	

Team Members:	**Grey Pawn 1**
Team Title:	
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	
Grouping 2	
Grouping 3	
Threat Actor or Adversary	
NOTE: Roll the Dice to pick a Threat Actor or Adversary (generally categorized by motive):	
1) State Sponsored	
2) Proxy	
3) Extremist/Terrorist/Hacktivists/Patriots	
4) No Specific Actor/Environmental	
5) Business	
6) Organization (e.g. political party, special interest group, religious group, etc.)	
Put your Threat Actor or Adversary here:	
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	
Where do they live?	
What is the threat?	
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
Who else in the person's life is involved?	
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	
What vulnerabilities does this expose?	
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	

Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Question Two	Answer your question in the yellow box
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	
2	
3	
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	
2	
3	
4	
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	
4	
5	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	

2	
3	
4	
5	

Team members:	**Red Pawn 2**
Team Title:	**Scarlet Witch**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	Tribalism becomes focus of IW operations
Grouping 2	Shared conceptions of reality
Grouping 3	Speech Modulation/Regulation
PART ONE: Who is your Person?	
can be anywhere...	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Bobby Jo, female flight attendant, visiting Athens Greece, 28 yr old, from Atlanta, based in NYC, the business class attendant for the Atlanta to Athens run, has friends and relatives globally
Where do they live?	from Atlanta, based in NYC
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	North Korea, state sponsor by proxy, to a Russian private bio tech company in Chinese crypto currency
What is the threat event?	fast mutating bio bomb launched at an airport hub for max distribution to global transit hubs - our flight attendent is patient zero, but the bioweapon is programmed to show know signs. She is our Typhoid Mary.
	"kill democracy where it began"
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	While in Athens, she is posting to instagram, she has a simple wifi spoof, her mobile device, and her biometric info ID is hacked. That contains her bio info security access. This is used to develop the weapon that turns her into the carrier - but shes carrying a digital virus in her biochip/augmentation. It is used to infect security personnel. Using her data to access airport systems, best infection vectors are pulled from security lines for enhanced inspection, propogating virus from security to civilians at scale.
Who else in the person's life is involved?	
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Targets the airport security system to manipulate the secure search; infect a fast moving virus to the TSA/security person; weapon is genetically bifenced to US citizens in FDA database, goal to unify Korea with North Korea at the head, and eliminating US resistance and removing them from global stage
What vulnerabilities does this expose?	we have a bio chip enabled population with biodata for all citizens; the implanted augments that create positive effects (deeper movie experiences, etc.) are virus factories waiting to be tripped; second phase of hack is psyops using the original Instagram account hack to deploy algorythims across social nets to (a) scrub mentions of the symptoms such that there is lower awareness of the disease and (b) create misinformation narratives about infected or uninfected demographics to drive blame, division and violence (e.g, 2030 census takers, dems or repubs, muslims, etc.)
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	

Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	first encounter at a popular bar/cafe in Athens, and comp[letely oblivious to the exploit. they'll not realize their digital exhaust was used to target them, that both their social and bio info were compromised, that the virus was custom-built to show no signs in her, but to fast mutate to avoid detection, and that digital feeds wont let info spread
Question Two	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	Coordinated mal/misdisinformation attack means virus spreads faster than truth: virus fans hate, differently affected groups feeds into multiple hate-based narratives ("well only dems are getting this") bio attack disables traditional medial forensics; secondary consequence is wealthy elite wiped out, suriviors are people opted or unable to be chipped (undocumentned immigrants survive)
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	spoofable wifi or connectivity; biochipped population and a centralized databaset; portable bioengineering devices; airports and key facilities using genetic and bio markers for ID; hiding activity from US cyber intrusion; relative genetic science
Question Two	Answer your question in the yellow box
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	Chinese Cryptocurrency, Russian Biotech; North Korean ransomware money; academic research funding
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	

What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	established intelligence network monitoring adversary networks
2	quantum encryption to defend biodata
3	redundant security agencies in major transport hubs
4	quarantine
5	securitized IOT/global protocols
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	**portable genetic engineering tools** to splice custom engineered viruses
2	implanted augments that translate digital info capable of generating physical/psychological effects
3	IOT hubs at the Edge/ Global IOT protocols
4	academic/medical research freedom/sharing of research info in non-security communities
5	freedom of movement/ global quarantining
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Enhanced security authentication protocols in addition to biometric, regulate the write privileges of the bio chip (specifics on what can and cannot be coded)
2	Global IoT Protocol
3	An effective World Health Organization mediated Treatise
4	Explore globally banning and penalizing bio-devices that produce physcological effect devices
5	Credentialing of IoT information sources (accredited media) to counter dis, mis, and malinformation
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Hardened augmentation... what is added to your body. Trust, how do we trust these devices? If we can be hit with a bio weapon, such as a sound weapon, then I can hack you from a distance to hack bio devices (the augments).
2	Develop technologies to update and patch the force's augmented (bio) devices from credentialed sources; rapidly
3	Develop AI/ML algorithms that analyze and identify anomalies/patterns within open source information indicating the creation and use of bio weapons that attack bio implanted devices
4	Create a system that protects research institutions IPs; create a framework for institutions to securely share research information; digital camouflage (can't see you, then they cannot hack you concept)
5	Develop a tool capable of recognizing modified DNA or genetic modification; example TSA scanner

Team Members:	**Orange Pawn 2**
Team Title:	**Pawntificate**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	Information as Center of Gravity
Grouping 2	News Desert: Natioanl news increase, locals news decrease
Grouping 3	We need to be prepared for fundamental attacks on the democratic processs via the information/digital domain. ((by definition: this would be attacks against 1) a political system for choosing and replacing the government through free and fair elections; 2) the active participation of the people, as citizens, in politics and civic life; 3) protection of the human rights of all citizens; 4) a rule of law, in which the laws and procedures apply equally to all citizens). Think about the weaknesses that are exposed through massive amounts of data about citizens / society that technology could exploit.
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	**Kasmer (internet shut off)** **US becuase not a lot of other contries donnot have local national** **Attacked** **federal action in local settings**
Who is your person and what is their broader community?	Joe Snuffy, Rural farmer, Citizens of rurual communities
Where do they live?	Taylor, Arizona
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	Offers from state actors in Mexico creating allies with Southwestern Farmers to potentially secede
Put your Threat Actor or Adversary here:	Mexico with Chinese/Russian help. The United States has been successfully countering Russian and Chinese information operations with AI and better cyber tools. However, since the completion of the wall, Mexico now sees the US as an adversary and the Russians/Chinese see an opening with Mexico as a proxy to get tanglible results from an IO. The growing secession movement in the US Southwest is seen as the perfect storm to break up the US by the three adversaries
What is the threat event?	Secession actions are local issues and these Local issues not making up into current ploitical enviroment/discussion
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Since 2019, Mr. Snuffy has been disenfranchised, political matters that are important the rural communities dont make it to national platforms. This is futher exacerbated by removal of electoral college and a recent push to increase senate to represent more populous states futher remove Mr. Snuff and hid confederates from their identity as Americans. A vote has been taken and is overwhelming in support of the succession and union /alligience with Mexico
Who else in the person's life is involved?	Children are looking to move to younger states where their voice will be heard. Community members and friends are advocating for taking actions to gain their own voice.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Offers from state actors in Mexico creating allies with Southwestern Farmers to potentially secede, Weaking of American Agriculture industry, National coverage would get more attanetion from the US govt
What vulnerabilities does this expose?	lack of quality local news in national platform keeps threats at local instution quiet.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	

What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
What is different and/or the same as previous events or instantiations of the threat?	The desire to keep the secession movement local and out of the national news to allow the critical mass to be achieved in time for them to accept the offer from Mexico.
Question Two	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	This local focused movement has implications for further division within the the United States with a real possibility of secession and possibly could spread globally, with nationalist movements growing stroger in Europe. This event could lead to the further breakup of the European union.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	Chinese disinformation campaigns to divide and weaken the US have thus far failed. However, with new policies such as the electoral college ban and the proposal to allow more Senators to represent larger states, the Chinese have seen an opening, via Mexico as a proxy, to get tangible results starting with a secession movement in Arizona and the SW United States
Question Two	Answer your question in the yellow box
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	Keep local avoiding social dumpster fires, win local governement and union, creating export markets that would benefit the communities better if run in Mexico. Natonal link in the SW to Defense indutry and need to seperate. Move to make NG and reserve force deploy to European fronts. The division of interests between the large population centers and SW need to be further exploited to position the SW for succession.
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	Platforms for Citizens Engagement
2	Acutuate Information Dissemination
3	Econmic controls and incentives
4	Civil Service
5	Education
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	Local Feeling /regional priorities
2	News Systems
3	WOM Campaigns
4	Digital communication paltforms
5	AI engines scrubbing keywords
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	

1	Locally important news shared nationally by National News services to provide empathy and understanding across the country to the unique regional concerns.
2	Reduciton of the radiciallized national policital news. The fear mongering is what other country would like to incite in our country and we are building on and assisting their efforts.
3	Education on media literacy and data literacy
4	Algorthims to currate the online news and identify and highlight incorrect imformation online.
5	Digital / online political town halls to discuss and familiar elecotrate with local government.
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Evalute digitial participatory governance
2	GOTV
3	Don't ban the electoral college
4	Adapt and adjust to our adversaries' strategies which grow and change as we do
5	

Team Members:	**Yellow Pawn 2**
Team Title:	**Goober versus the Family**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	liars dividend
Grouping 2	complicent in targeting
Grouping 3	Closing income, education, and inequality gaps is the only way we can insure competitiveness and full participation in IW
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Carmine Santino, son of one of the 5 families; age 20, supervises logistics systems at the docks
Where do they live?	Newark, New Jersey
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	District Attorney is running a campaign against the Santino family, wanting to reign in corruption; doesn't understand the connections that the mob controls; using AI to generate the entire video content; Young & idealistic DA plus a very public push for "Goober" (Uber for sustainable trash pickup) is a sensational idea generating lots of campaign money for public officers who support it.
What is the threat event?	Deep fake video shows his father at fund raising dinner and links to other phones at the same event showing the same video talking about screwing over the sanitation workers; threat is that by taking down the crime family interupts sanitation/garbage collection,
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Carmine has to figure out how to counter the deep fake video IOT reassert his Family's control over the garbage industry without causing shame, without doing something (too) illegal, and needs to prepare for the next wave of smear the DA's office is about to release
Who else in the person's life is involved?	Carmine's cousin Sylvia is a computer science student at Columbia U, interning at New Jersey DA for a semester. She tips him off that the DA is prepping a larger smear campaign than this first video. Sylvia got her internship because of an AI-enabled search that selected her from 100,000 candidates of computer science students in the greater NYC metro area, based on analysis of her public and semi-public ("data exhaust") profiles AND a requirement to select diverse candidates.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	DA wants to undercut the influence of the Santino family as part of the office's fight against corruption and mob control over economics
What vulnerabilities does this expose?	how unseen/ignored actors influence daily life; this is an example of "reflexive control" meaning forcing the son (Carmine) to act in a way favorable for the DA is a way to control the father and the Family

PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
What will this make your person do that they normally would not?	He will have to reveal his capabilities to access the internet and spoof biometic data that are outside of the legal means of accessing the internet; Even though Carmine approached his dad to confirm the video was fake (because no one trusts videos anymore), his father told him not to take any illegal action (hacking). Impulsive teenagers/young-20s want to show how he protects the Family.
Question Two	Answer your question in the yellow box
What is different and/or the same as previous events or instantiations of the threat?	to counter this, he will have to hack all the original gadgets the state drew on to develop the AI fake and push the unaltered video
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	Internet use/ commerce/credit system is tied to biometric data; burner phones illegal; highly connected devices are vulnerable to AI attacks to turn on multiple devices in a particular area, capture video/audio, and re-create an AI-generated environment for DEEP, deep fakes
Question Two	Answer your question in the yellow box
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	Data privacy law has taken effect which has then subsequently reduced anonymity of data. The legal environment has taken away civil liberties that makes government surveilance of individuals devices easier by tying internet enabled devices tied to biometric markers. The Supreme Court has reinterpreted privacy to individual not their devices or data.
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	

Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	(I.e. things the FAMILY controls)
1	Loyalty - controls clean sanitation services for the cities which builds good rep with citizens
2	Coming/going of people within trust circles in the family; they can choose who is put in certain areas
3	Need to have access to secure tech that bypasses requirement to tie personal IDs to devices (i.e. biometric spoofing or anonymity tools - probably illegal now)
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	DA in enforcing the law, has to go against public opinion and upset the Family' s good rep with citizens
2	Privatizing of public services such as "Goober" (Uber for sustainable and eco-friendly trash pickup)
3	Speed of AI technology - dual use
4	Amount of garbage mob's trash system was picking up is being reduced by environmental impact measures and improvements (i.e. back to highly recyclable containers, which feed the demand for 3D printing raw materials)
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Rapid development in recycling advancements - repurposable recyclables, esp. for 3D printing
2	Rapid improvements in AI that can create entire environments out of scratch, rather than deep faking a face over another actor in an existing video
3	Robots capable of separating old electronics increase the profit margin for recycling tech
4	
5	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	National data protection law passed (i.e. pseudo-GDPR) that also requires individuals to be tied to their devices - anonymity reduced
2	Children's biometric/DNA data can't be legally collected until they are 16. Kids are finding ways to get online without this DNA verification. Tech is secretly developed to support the illicit anonymity market.
3	
4	
5	

Team Members:	**Teal Pawn 2**	
Team Title:	**Huawei Go**	
Estimated Date of the Threat:	**2029**	
Data Points		
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)		
		dice rolls
Grouping 1	Information is center of gravity	13
Grouping 2	VR / Immersive content	7
Grouping 3	Fragmentation of personal realities	11
PART ONE: Who is your Person?		
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.		
Who is your person and what is their broader community?	Kaspar: Systems Admin / Developer for the major AR/VR corporation (off shoot of Huwaei). out-sourced worker; 30 years old; ran a fraudulent ICO scam in the past that screwed Estonia; lives alone with a pet rock	
Environment details:	AR - immersive environment that is personalized for individuals/communities; evolution of Netflix (infinite content available that is personalized to what you want); this becomes the battleground for the proxy war between India and China; AR gaming envionrment took off on Africa continent. given state of smart phone technology on the continent - makes this capable. compelling AR content is a mixture of gamified content and IRL competition. The content heavily relies on "the others" which motivates players to attack / gain an advantage over another group. The motivation for the game depends on motivating users against a perceived outsider threat that usually takes the form of unfamiliar strangers. Once the exploit is carried out, the opponent group becomes modifiable by attackers, and thus the motivations and emotions of users can be tailored against any group. India realizes this can advance their "hearts and minds" campaign against China and thus motivate local sentiment in their favor.	
	US lost the trade war with China and are forced to allow Huwaei phones into the US. Resulting market share is that they are more popular than Andriod or Iphones. The US market is flooded with these devices.	
Where do they live?	Estonia	
Threat Actor or Adversary		
NOTE: Pick a Threat Actor or Adversary:		
1) State Sponsored		
2) Non-state Sponsored		
Put your Threat Actor or Adversary here:	Indian state operatives (hackers, info war planners)	
What is the threat event?	A concerted effort to blackmail Kaspar in order to access and manipulate the core AR/VR alogirthm w/o the Huawei's knowledge.	
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	He was the developer behind a massive ICO scam that crippled the Estonian economy as they left the EU. Because flipped on his co-conspiritors interpol kept his identity secret and none of his immidiate network knows what he did.	
Who else in the person's life is involved?	His immediate family is wrapped up in the Estonian nationalist movement. Extremely anti-EU and blames them for the economic collapse. His developer network is actively engaged in anti-EU activities.	
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Sow civil unrest in the African continent to counter chinese successes. Specifically targeting African politicians and their families. Expose / frame African politicians as Chinese proxies. Creating dis-trust in the Chinese infrastructure that underpins their lives.	
	proxy war	
What vulnerabilities does this expose?	There is no way to determine the physical truth. Human vultrabilities in even the most secure technology.	
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)		
Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?		
What will this make your person do that they normally would not?		
What is different and/or the same as previous events or instantiations of the threat?		
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?		
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)		
What will the person have to do to access people, services, technology and information they need?		
What are the broader implications of a threat like this? What might a ripple effect look like?		
Question One	Answer your question in the yellow box	

"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	Indian hackers turn Kaspar by threatening to expose him for his role in the collapse of the Estonian economy. They push him to open up a door for them to inject their propoganda into the feeds for a two month period leading up to a big event.	
Question Two	Answer your question in the yellow box	
What are the broader implications of a threat like this? What might a ripple effect look like?	Once the vulnerability is created it becomes a known exploit amongst hackers throughout the world. The vulnerable phones are in US and EU using the immersive content drive a massive amount of people into a known location. And given the love of the immersive event, they wont get off it even knowing that it is compromised.	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)		
Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?		
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?		
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?		
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?		
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?		
Russian/China/Iran/N. Korea (Big 4) culture/politics placeholder question		
Question One	Answer your question in the yellow box	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	Off-shoring development was a norm, creating broader networks of individuals with access to the technology. Less people around him to notice eratic behavior (because off-shore developer). Not enough oversight.	
Question Two	Answer your question in the yellow box	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	Immersive content getting better, PokemonGo on steroids: social status and monitary insentives integrated intop the game. Smart phone and 5G improvement allows for Huawei phones to enable these experiences. Longer battery life enabling extended experience.	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)		
Examine the combination of both the Experience Questions as well as the Enabling Questions.		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.		
1	Corporations tightly control access to and the development of feeds / algorithms, oversight by regulators	
2	Transparency in the algorithms and operating systems of mobile devices makes it harder to hide malicious code / updates in plain sight	
3	Data literacy increases through a function of generational change, increased skepticism of social media and extreme online content	
4	Continue to prevent Chinese + foreign government consumer hardware from gaining traction in the West	
5	Manhattan-style project bringing together industry + software experts to regain control of this broken arrow immersive conten	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	The immersive content industry has legs and there are more than a handful of Pokemon-Go style successes – If Pokemon Go is Friendster, then there's some evolved version that has increased complexity and engagement ala Facebook	
2	Increased opacity of the algorithms directing people's behavior IRL, and a decrease in corporate desire for transparancy	
3	Decrease in domestic workforce, increase in off-shore developers with greater responsibility over core business logic and algorithms	
4	Proxy battles between nation states increase in the information realm – India and China decide to fight it out with information not kinetics	
5	Huawei winning access to the American market	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Discussion of transparency in aglorithms, funding for research of black box algorithm insight – NAS could fund researchers who work alongside social media company engineers to help public understand algorithms. GDPR-style audting of the algorithm's outputs is more important than its internal workings. Expectation that companies are protecting their secret sauce.	

2	Government level support for teams to understand algorithms; decreased liability for more transparent algorithms	
3	Investing in research that identifies effective tools and education for increasing digital literacy that can be handled to non-profits to be dissiminated ala international aid currently	
4	Digital blue helmets: reserve engineers + scientists + sociologists willing to help foreign nations and other organizations mitigate damage caused by weaponized content and algorithms	
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Former tech executives and engineers end up with public servant roles and have a vastly deeper understanding of how to regulate and legislate algorithms both domestic and foreign	
2	Information warfare geneva convention established, able to identify China and India as violators	
3		
4		
5		

Team Members:	**Purple Pawn 2**
Team Title:	**Purple Haze**
Estimated Date of the Threat:	**2029**

Data Points

NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)

Grouping 1	Science says frontal cortex not fully formed in males til 25 - how are males under 25 more of a target from 1st data point
Grouping 2	In crisis: no idea where to get their true news
Grouping 3	connection of the fringes

PART ONE: Who is your Person?

NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.

Who is your person and what is their broader community?	Kanye West - People of Color, Millenials, and former mainstream Trump supporters, leftwing voters
Where do they live?	Primarily on left right coasts of the US, but also in Gulf Coast region for the first time.

Threat Actor or Adversary

NOTE: Pick a Threat Actor or Adversary:

1) State Sponsored

2) Non-state Sponsored

Put your Threat Actor or Adversary here:	Kanye West
What is the threat event?	Kanye narrowly loses 2028 election by .5% and declares election results subject to fraud
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Refuses to stop legally and socially contesting 2028 election results similar to Bush v Gore 2000. Organizes supporters to march on Washington DC in an organized protest that brings transportation, economic activity, and federal functions to a halt.
Who else in the person's life is involved?	Donald Trump who supports his friend Kanye, and Kim Kardashian.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	To cause a Constitutiuonal crisis. To lead a political fractionalization of the US along ideological-cultural lines. That a public backlash of these events will galvanize national unity and patriotism in the US.
What vulnerabilities does this expose?	Cultural, social, economic, political, and geographic fissures in the US.

PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)

Questions (pick two) from the drop down selections

Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>

"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?

What will this make your person do that they normally would not?

What is different and/or the same as previous events or instantiations of the threat?

When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?

How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)

What will the person have to do to access people, services, technology and information they need?

What are the broader implications of a threat like this? What might a ripple effect look like?

Question One	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	So the US can no longer act as a a global hegemon or leader for the West in international politics due to the fact that a fractured confederacy will not have the economic or military power to project as it currently does.
Question Two	Answer your question in the yellow box
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	Kanye West's campaign team uses personalized vignettes that conform to individual voter beliefs and preferences that are only delivered to an individuals' personal news and information feeds via advertising, social media, and print media. This prevents his coalition which is naturally internally fractured from fracturing, by never disclosing controversial policy stances or opinions from each other. Publicly, Kanye supporters only see valence issues, stances, or messages in public events where cross contatminations of information streams could occur - eg campaign rallies, protests. Additionally, public events not intended to cause chaos are carefully curated in who attends them in order to prevent friction between groups of supporters in public. Essentially, alternative facts have become alternative realities.

PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)

Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?		
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?		
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?		
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?		
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?		
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question		
Question One	Answer your question in the yellow box	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	1, Electoral college willl and should serve as a saftey net to prevent this issue, but it is undermined because multiple states across the country where the popular vote was within %0.1 have a number of faithless electors that do not conform to the popular vote in each state. Principally in Texas where Kanye wins the popular vote, but three electors vote for the Democrat incumbant. 2, The US Military/Law Enforcement/DHS serves as a barrier to the splintering of the US and the dissolution of the current constitution by enforcing martial law on behalf of the incumbant and to support adjudication of the election within the courts. 3, Hacktivists bring down contemporary media streams and interfere with personalized media content to present broader media picture to general public to dilute alternative information realities.	
Question Two	Answer your question in the yellow box	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	Personalized nano-targeting of audiences as blue and red as only version of reality, news, content (based on self political party identification). Whole room OLED screens in homes (the transition from living room to a media room) to create "virtual reality" and have the PResident talk with you, play games with you...brings new meaning to term "candidate can have a beer with". Reality is altered based on your political identity.	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)		
Examine the combination of both the Experience Questions as well as the Enabling Questions.		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.		
1	Institutions of government - military, supporters of traditional constitution and whole of U.S.	
2	Media elite - all formats	
3	Local Community - strong communities will diminish personalization effects	
4	Big Tech	
5		
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	2000 Bush v Gore - Palm Beach County, Hanging Chads	
2	2016 Election - Trump mainstreams the concept of Fake News and publicly begins undermining confidence in the impartiality and veracity of	
3	2016 Final Presidential Debate - Clinton asks Trump if he would abide by results of the election; Clinton loses, Democratw begin discussion undermining the legiticmacy and purpose of the Electoral College	
4	Circa 2016 Kanye West aligns himself politically with Donald Trump	
5	Trump appoints Kanye as ambassador to Russia; Dennis Rodman to North Korea	
6	Voting goes to online only with fingerprint as identity proof	
7	2025 Trump formally endorses Kanye as Presidential candidate.	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	Trump loses 2020 re-election bid and peacefully transitions government.	
1	Convention between big tech and governemnt on ethics in media framing and delivery of	
2		
3		
4		
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1		
2		
3		
4		

Team Members:	**Black Pawn 2**
Team Title:	**October Suprise 2028**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	Tribalism becomes focus of IW operations
Grouping 2	Generation born into curated, personalized content have no resistance, resilience or immunity
Grouping 3	200 years of Democratic institutions being attacked
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Jackson Marsh, African American, Denver Police Chief
Where do they live?	Denver Colorado USA
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	China
What is the threat event?	China is facing a sustained Economic downturn, and decides to use AI and ML to disrupt the American voting process
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	China micro targets US individuals inflaming passions and inciting support/organizing along "tribal lines" ANTIFA , BLM and local KKK affliated groups to start a misinfomation and disinformation campaign centered around voting thus giving rise to fringe party elements and those specilizing in identity politics
Who else in the person's life is involved?	The Chief is African American, also affected is his White Wife and his Bi Racial daughter that is attending college in NYC.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	China is seeking to create widespread chaos, distrust in an effort to suspend or delay the upcomming Presidential Elections - first time in US history. China wants to keep the incumbent administration in office.
What vulnerabilities does this expose?	Election Security, technical vulnerabilities of Social Media, Confidence in democratic insitutions.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	Chief Marsh's daughter contacts him informing him that she has been notified via social media that large numbers od African Americans have been killed by White White Supremist elements. Also, his daughter has seen deep fake videos of African Americans being lynched in the Denver area. She wants to come home and defend her friends and family.

Question Two	Answer your question in the yellow box
What will this make your person do that they normally would not?	Chief Marsh is torn between family and professional responsibilities. His family is strained by ethnic tensions and tribalism - he personally looks forward to the federal election to bring leadership and stability, but the federal govt has announced the delay of the federal elections for a minimum of 12 months, a decision he is personally responsible to support and enforce. Chief Marsh comes out in public opposiiton to the President's directive to delay elections and gains backing/support from the Colorado Governor (R) who announces that Colorado elections, including Federal ballot issues will be held using paper ballots. Following Colorado's lead states split in support or opposition to the (D) President's decision to suspend elections. Colorado Governor mobilizes the Colorado National Guard to ensure elections are held as scheduled. New York mobilizes their Guard to ensure elections are not held.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	Micro targeting essentially possible today, its the Macro scaling that is not feasible yet: AI/ML, neomorphic computing not mature enough, network latency, not enough data scientists, and other resources to effectively influence individuals at scale.
Question Two	Answer your question in the yellow box
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	Crowdsourcing, the increased viability of anonymity computing, also additional AI/ML education programs available for free which have created hundreds of thousands of developers who are incentivized to unknowingly providing innovation to the Chinese government.
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	Government Regulation Restricting Tech to China
2	Govt Regs ensuring Ehanced Security software embedding technology to succesfully detect deep fakes, companies must demonstrate and certify their due diligence in keeping fake news/deep fakes off their platforms.
3	Fall back planning to include low tech solutions such as paper ballots avail.
4	"Compute Kill switch" Committee - controlled by a non-partisan, cross-sector, diverse public-private stakeholders.
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	The Speed of the growth of technology and the unregulated advances in personal computing
2	Increased social Tribalism
3	Racial Tensions (nationally)
4	Educational inefficency leading to increased
5	The next technology that we cannot anticpiate/ non state actors/ new political parties
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	

4	
5	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Increase Diversity of thought in Govt ,Industry and early childhood education
2	
3	
4	
5	

Team members:	**Red Pawn 3**
Team Title:	**Scarlet Witch**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	movement to violence
Grouping 2	AI chatbots for radicalizing dialogue
Grouping 3	information as center of gravity
PART ONE: Who is your Person?	
can be anywhere...	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	MAJ Diego Garcia, S2, intelligence Officer, Brigade Combat TeamM
Where do they live?	Deployed to Madama, Niger, Africa (only city in NE Niger bordering Libya to the North and Chad to the East)
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	China by proxy using radicalized groups out of Libya and Chad; China has large investment in Nigerios Oil and Hydro carbons. Niger is also deeply indebted to China as a result of loans for infrastructure projects. The Niger government is disintegrating under the weight of Chinese debt. The debt crisis has consequentially caused an Humanitarian crisis within Niger. As a result the international community, under the supervision of the U.N., has assembled Humanitarian Relief Operation to help Niger. These events have caused China to lose influence and substantial financial investment in Niger. MAJ Diego Garcia's brigade represents the U.S.'s support in this effort. The U.S. mission is to stave off humanitarian disaster and desolve Chinese influence in the nation. China's goal is to weaponize information in an effort to cause the U. N. task force's and more specifically the U.S.'s mission to fail.
What is the threat event?	Coordinated digital and PSYOPs campaign to force MAJ Diego's brigade to withdraw from Madama without using controlled violence. Deep fake video's of U.S. Soldiers raping Nigerois woman and of U.S. security contractors summarily executing a remote Nigerios village (burning the village) on the outskirts of Madama which are proliferated through AI controlled chat bots on Chinese supplied 5G architecture. The most profound deep fake video depicts the beheading of a U.S. Soldier. This event both inspires local radical groups and creates dissent at home. The Chinese own and controll the information infrastructure which is leased to Niger. Huwai equipment are used in this infrastructure.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Diego a mass of Madama citizens violently protest outside the brigade's base camp. A sniper from within Madama wounds a soldier during a presence patrol. Evidence of radicalized militant groups capable of enacting violence is appearing with intelligence reports from higher headquarters. China is creating virtual radical groups using virtual botnets that create solidarity with actual local radical groups inspiring action from them. The virtual radical groups are driven through AI driven botnets that uses digital exhaust, measures sentiment, and adjust its narrative without the intervention of humans. Deep fakes are timed to coordinate with supporting events such as farmers burning their fields after the normal harvesting process.
Who else in the person's life is involved?	Wife and children back home are scared. The children are crying and asking if the person in the video is their dad. U.S. public sentiment is becoming overwhelmingly opposed to the operation.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	China's goal is to weaponize information in an effort to cause the U.N. task force's and more specifically the U.S.'s mission to fail. Strategically China is looking to preserve their hydro carbon investment, long term secure rights to uranium deposits in the country (the world's largest). Prevent a restructuring of the Nation's debt (IMF bailout).
What vulnerabilities does this expose?	Secure encrypted information infrastructure (quantum) preventing a look at what is going on inside Niger. The Brigade's network for bandwidth purposes would have to connect to information infrastructure controlled by our adversary or competitor in the region. Authorities for capturing local social media data and higher presence on networks. Local's knowing we monitor their networks; however, due 5G technology they are able to create mobile ad hoc mesh networks that not trackable.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	

Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>		
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?		
What will this make your person do what they normally would not?		
What is different and/or the same as previous events or instantiations of the threat?	Technological advances in 5G architecture, quantum encryption, the ability to automate high-quality, multi-view point,fake video, audio, and narrative	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?		
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)		
What will the person have to do to access people, services, technology and information they need?		
What are the broader implications of a threat like this? What might a ripple effect look like?	It could cause de-stabilization in the U.S. Cost of deployment is greatly increase based on the technology (deploying the network), combat networks using organic 5G technologies that support not only troops but the local government and population. The use of AI technologies that cause ethical concerns and may compromise U.S. ideals. How do you properly credential US forces deployed to validate who you actually are, example distinguish between real and fake videos in the view of the local population?	
Question One	Answer your question in the yellow box	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?		
Question Two	Answer your question in the yellow box	
What are the broader implications of a threat like this? What might a ripple effect look like?		
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)		
Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>		
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	Deploying and installing 5G architecture into a remote area like Madama is costly and cumbersome. They lack emotional and conscious (empathy) intelligence for establishing meaningful human relations with the local population. Cultural differences create obstacles geographically. Local and Niger government is resistant to Chinese influence.	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?		
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	Next generation entertainment models powered by 5G, customized by persoan preference models. Chinese cultural export and money influences local culture, improves local living conditions.	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?		
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?		
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question		
Question One	Answer your question in the yellow box	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?		
Question Two	Answer your question in the yellow box	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?		
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)		
Examine the combination of both the Experience Questions as well as the Enabling Questions.		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.		
1	Develop mobile 5G information infrastucture (deployable). Portable controllable cyberspace.	

2	Credential troops to distinguish between fake and real content (audio, video, and narrative).	
3	Authorities to monitor flow over local information infrastructure	
4	Develop the ability to detect 5G mobile ad hoc mesh networks	
5	Signature management - the ability to monitor our own digital exhaust and media output. example Diego post a geo-tagged pictu	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	Classic man-in-the-middle attack; Adversary controls the infrastructure - manipulate digital traffic between deployed force and home	
2	Chinese space based systems - what they can see and analyze	
3	The gap between the physical environment boundaries (geography) and boundaryless virtual environment	
4	encrypted networks	
5	Don't have control over local history	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Develop portable, cost effective, deployable 5G communications architecture	
2	Organic human terrain teams (uniformed)	
3	Electonic warfare capabilities to detect ad hoc 5G networks	
4	AI driven deep fake content detection	
5	Virtualized units whose job is to produce local knowledge; secondarily create a conceirge like service to provide virtualized information to local populations based on local technologies; awareness and monitoring of local services	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Augmented reality for MILDEC purposes; deception to quell violent protest; fool satellites	
2	Unbreakable encryption (quantum encryption?)	
3	Enhanced ability to validate networked communications over non-controlled (non-American) information infrastructure. Blockchaining, ledger technology for validation (non-repudiation)	
4		
5		

Estimated Date of the Threat:	**Orange Pawn 3**
Team Title:	**Not Really There...**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	escalation models
Grouping 2	one-on-one marketing relationships
Grouping 3	Manipulation in augmented reality
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	**training polish fighters on immersive technologies**
Who is your person and what is their broader community?	Joe Snuffy an E-7 in the US Army, Polish Military and other US Support personnel
Where do they live?	Rotationally deployted to Fort Trump, with family at Fort Bliss.
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	Information Operations Units within the Russian Federation.
What is the threat event?	VR training exploitation by Russian operatives that actively recruit, threaten, and solicit our Polish partners. Russians are able to do this via data harvesting from social media platforms
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	One-on-one specialty targeting in the VR domain has effective psychological impacts on these individuals that can begin to wear Polish perceptions of the US
Who else in the person's life is involved?	Soldiers immediate and extended family within El Paso, and throughtout the midwest.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Sow dissent between the Polish and U.S. trainers as well as targetting psop attack against the Soldiers state of mind, with the goal of inducing depression and also distrust of the agumented VR systems, and making training ineffective. The goal is to create discontent between the US and Poland, attract the Polish to Russia, and degrade and demoralize Western fighting forces via VR exploitation. The Russian ability to degrate the forward units and regain Polish suport and look to moving along and resizing all the Baltics.
What vulnerabilities does this expose?	Connected VR systems that are interconnected as well as increased ability for the immersive enviroment to do individual damage to Soldiers and to create individual worlds that degrade the commanality needed for training.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	

Question One	Answer your question in the yellow box
What will the person have to do to access people, services, technology and information they need?	To create a personalized user experience tied to a user login on a VR machine. Blend the targeted messaging to the default programming so to the user cannot identify that they are being targeted
Question Two	Answer your question in the yellow box
What will this make your person do that they normally would not?	The subliminal messaging able to be achieved via VR platforms is slowly transforming Joe's thinking about Poland, the Polish, and those he is training. The same is happening with Polish soldiers and their thinking about the US
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	Threat actor is going to need to know in detail what is normal at Fort Bliss, as well as Fort Trump. Will need to understand the social concerns of the Polish Soldiers as well. Will need to understand how the VR systems works and be able to enter the system and how it is interconnected. Social engineering ot the Polish Soldiers that have been trained.
Question Two	Answer your question in the yellow box
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	Need local infrasture within Poland to inflitrate the VR systems. Criminal elements with Poland are enticed to provide the required infrasture. As well, the Russians will begin to court the Polish government and attempt to influence the Polish soldiers through their VR systems.
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	Security systems within the VR and risk management frameworks
2	Social Media filtering for Military and American Families
3	Fund studies on the psychological impact of VR tech on human beings
4	Dedicated instrusion detection within the VR environment
5	Good education for users as well as trainers.
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	Foreign allies and relationships
2	Effectiveness of a VR campaign on Soldiers and Allies
3	Private sector funded tech with military adoption and possibly infilitation of the supply chain earlier in the process.
4	Cost of being an early implementer or adopter. Where on the adoption curve is the technology we are using for training.
5	Don't have influence over the targets of our enemies
Milestones:	

What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Develop security for indivudualized training technologies
2	Proactive in adoption standards to ensure tech is at least knew to the hackers
3	Better visibility and connection of deployed Soldiers with their families to reduce the target for misinformation and possilbe exploitation
4	Expectation managment of the training benefits of training environments and understanding the potential shortcomings of our service members.
5	Enlist the industry partners to secure the supply chain during early research and adoption
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Norm development with like minded countries to mitigate bad behavior in the information domain
2	NIST type standards and regulations for sercurity in the VR environment and design the tools that will help troubleshoot
3	Ensure that VR training is considered important training and not considered an afterthough to ensure that Soldiers understand how the systems work, but also can identify anomolies.
4	Need to finds ways to incorporate the cyber and information training pre deployment and ensure clean environments have been identified prior to deployments
5	Establish Central Data clearing house for Operations Research into the Virtual domains and the intergration of training among allies within these new technologies

Team Members:	**Yellow Pawn 3**
Team Title:	**Imperial Beach**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	reflexive control
Grouping 2	virtual reality and information spread /immersive content
Grouping 3	Issues of free speech are no longer just the providence of individuals or governments. Corporations have a vested interest in this issue and can influence where societies head. (example Facebook)
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	SGT Maria Sanchez, a Puerto Rican American, who was turned away from the border during Hurricane Maria in 2017, later enlisted in the Army, but still is bitter at the Trump administration for spurning Puerto Rican support requests. She is deployed to the California/Mexico border just south of the now underwater Imperial Beach area. During her work shifts, she controls a security checkpoint that receives dozens of live sensor feeds into a VR environment. Her rules of engagement allow her to fire upon any non-registered watercraft identified by the system entering into the contested waters.
Where do they live?	Deployed to CA/Mexico border but lives at Fort Hood, TX
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	A paid hacktivist that supports the movement for California to secede from USA
What is the threat event?	Federal troops “accidentally “ fire on a mexican military border patrol boat due to a cyber attack on the US military person’s VR display and takes advantage of rules of engagement system difficencies.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	SGT Sanchez’s VR suite displays a watercraft that appears within the contested waters and registers it as a legal target for lethal engagement, because it has fully crossed the international border improperly. However, the system has been hacked to put a “okay to shoot” tag on a Mexican boat that is within its own territory.
Who else in the person's life is involved?	Her commander believes she acted correctly but there is a 15-6 investigation and in this process CID cyber analysis is finding conflicting and incunclusive evidences of cyber hacking on the SGT’s VR recording device. Files that should be stored are missing and while SGT Sanchez is fighting for her innocence inside UCMJ, some national media are putting her actions on trial in the court of public opinion.
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Want her to be the fall person. Want to push the rhetoric that California and US Federal system are incompatible, and sow public distrust.

What vulnerabilities does this expose?	Undermining trust in digital military network and battle space visualization tools for Military personnel. Undermining social trust in political leadership at local, state and federal levels. Undermining the international trust and agreements between Mexico, US and California. Racial and ethnic divides fuel mixed emotions for the fate of SGT Sanchez.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	Coast lines shrink as climate change causes sea levels to rise. California is disgusted with Federal response to disasters on Caliornia coasts and groups begin movements to secede from teh nation. SGT Sanchez has all teh same physiological and psychological manifestations that occur whenever anyone is asked to make a decision to pull the trigger and end someone's life. She also is feeling certain about her training on the VR sentry system, and has a hard time believing that such advanced tech could be wrong. She has feelings aboutte trust between her and her command as well as previous feelings of mistrust towards the federal gov't when she wa a child, nd now she is being thrown under the bus of public opinion by the federal gov't again.
Question Two	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	Broad implications of trusting digital tools in military decision making; dependence on civilian (or dual-use) telecoms architecture continues to reveal vulnerabilities of access to military systems; in the scenario, this inflames the resolve of pro-secessionist supporters for California to leave the nation. An external actor convinces her that they can help her examine the VR system to find the truth, but this is another layer to open vulnerabilities into military systems.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box

Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	Inividualized and personal VR systems for each soldier that can be connected to the greater C2 or mission command networks; glide path for greater high speed broadband must continue and spectrum management must allow for wirelessly connected VR systems; VR transport (compression, etc) must develop so processing can be at the edge (at the individual soldier)
Question Two	Answer your question in the yellow box
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	A hactivist would probably need insider access to either SGT Sanchez's personal system (i.e. close personal access), to the connectivity backbone (i.e. thru wireless tech intercept), or through the public telecoms transport system; hactivist would also need massive support from pro-secessionist movement to ensure his actin were in line with their agenda
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	Rapid acquisition processes to field high-tech to soldiers and increase interoperability
2	Selection of companies who develop tech for military applications
3	
4	
5	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	States refusing to send troops to the borders in support of federal policies
2	President has to regain control over Right Coast Revolt; using federal troops is one tool - she has others
3	Insider actions / insider threat is still not perfectly mitigatable
4	
5	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Trade tariffs, data privacy requirements, intellectual property requirements have begun bringing tech development back to the US —> leading to slightly increased control and trust over US-made tech
2	Anything to do to address climate change issues
3	Federal gov't no longer subsidizes flood insurance for at-risk locations due to rising coastal waters
4	
5	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	AI-enabled scanning of networks for intrusions and hacks becomes more common

2	Federal acknowledgement that we did Puerto Rico wrong in the lack of support after Hurricane Maria
3	Education and emphasis on patriotism and national pride
4	Mechanisms (of whatever type...) to increase trust in democratic institutions
5	

Team Members:	**Teal Pawn 3**	
Team Title:	**Therapist Ready to Talk (TRT)**	
Estimated Date of the Threat:	**2029**	
Data Points		
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)		
		dice rolls
Grouping 1	AI chatbots for radicalizing dialogue	8
Grouping 2	Complicit in targeting (everyone is ok with being targetted)	4
Grouping 3	Military advantage evaporates in 2030; boundaries; dissolution of boundaries	3
PART ONE: Who is your Person?		
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.		
Who is your person and what is their broader community?	Samantha, National Guard Soldier who is activated by the governor to quell unrest. She lives El Paso, Texas. Family situation? Her normal job is a social worker for the state ... this is "fringe-automatable" so worried about evolution of tech and the Chat Bot.	
Environment details:	US is more isolationist. We have lost our military advantage in the world. we are focused on keeping the peace at home now. nation states all have AI that puts us all in a stale-male for first action. Still dominate in nuclear capability but the battlefield with respect to information warfare / cyber we no longer have the advantage. Emotional therapy chatbots are military issue for all deployed personal to manage their mental health and be proactive about PTSD. Managing anxiety about conflicting feelings brought up by being deployed inside the US against our own citizenns	
	In 2024, Texas went blue. There is civil unrest and the Governor calls in the National Guard to maintain order in Austin. Since we lost our positioning in the world order, we are also losing out on trade agreements which is generating more anxiety and issues within the US	
	This mental health chatbot (Therapist Ready to Talk) was originally designed as a great idea. The ability to provide customized and personalized mental health assistance to troops while deployed. Something private that could assist them when they are in conflict. It starts out very successful and then individuals start to realize its potential and power to influence.	
Where do they live?	Deployed in Austin Texas	
Threat Actor or Adversary		
NOTE: Pick a Threat Actor or Adversary:		
1) State Sponsored		
2) Non-state Sponsored		
Put your Threat Actor or Adversary here:	Hyper-politsized General. Hawkish on his belief in 'Real American Values', dedicating himself to get Texas to go back to Red.	
What is the threat event?	Altering the mental health chatbot ... to start polarizing troops vice helping them. All in an effort to regain Texas on the red side of the political spectrum. Scary situation where the adversary is ourselves (i.e. US troops against US citizens).	
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Samantha realizes there's a change in tone with the army supplied chat (TRT, Therapist Ready to Talk) and is worried that it will exacerbate the divisions between civilians and the National Guard. There also is an increase in conflict within the National Guard unit as some are pro the civil unrest and some are anti. Troops engage citizens and citizens are shot. Samantha goes back to her chat box to help her deal with it and the chatbot seems to rationalize the killing of US citizens	
Who else in the person's life is involved?	Top commander is complicit influencing TRT	
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Decisive victory through increasing the brutality and suppression inflicted by the National Guard – martial law until the state can be redistricted and secured a Republican win	
What vulnerabilities does this expose?	The risk of politics influencing high level resources within the army such that a commander etc could control or manipulate a chatbot to change people	
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)		
Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?		
What will this make your person do that they normally would not?		
What is different and/or the same as previous events or instantiations of the threat?		
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?		
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)		

What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	Troops engage citizens and citizens are shot during a protest. Samantha goes back to her chat box to help her deal with it and the chatbot seems to rationalize the killing of US citizens as the adversary instead of properly helping her deal with her internal conflict.
Question Two	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	The accumulated effects of the chatbot result in a severing of the armed force's sense of civic duty – they no longer see citizens as people to be protected but rather the advesary to be defeated. This makes sense because over the last 8 years, this system as been tested and rolled out to the force. Therefore, every Soldier has a chatbot and is trained to talk to it.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	
Russian/China/Iran/N. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	AI becomes seen as a solution for mental health issues both privately and publicly as the next evolution of telemedicine. Recommending chatbots instead of IRL talk therapy becomes easier and cheaper and the military embraces this as a fast solution to growing concerns around mental health. Government contractors eventually specialize in military-specific chatbots that repurpose trends in civilian psychology. Initially these are seen as good developments lowering the cost of medicine and treatment, but they how they work and at what scale opens them up for abuse
Question Two	Answer your question in the yellow box
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	Due to decreased economic opportunities more people enlished in armed services, while others cannot find employment increasing social unrest and disenfranchisement. This increase the likelihood of civil conflict between domestic armed forces and civilians, AI acccelerates the division by automating the resentment between the groups
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	Maintain truth and belief in the political process. So, that if a state changes colors - it is accepted as the truth and belief of its citizens. ((to keep it from turning into civil unrest when it would change))
2	Unify language in the political discourse. unifying American narratives are needed to be crafted and socialized. This would make us more tolerant.
3	Passing campaign finance reform. This would support the idea of unifying language by deinsenscentivizing devisive political discourse
4	Board of medical and mental health doctors that oversee and approve changes to the chatbot. Also need to consider the need for physical interaction and relationships when dealing with mental health. Make it an FDA device.
5	Dont politicize the military
6	Providing alternative models for wider segments of the country to participate in defending the nation - serving their country and the military. Increase the definition within the military about what is "service". this would provide a more balanced respresentation of what the country's beliefs are within the military.
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	increased domestic terrorism. less lone wolves and more cells (militias, etc). continued narrative from the government that they are not as important to fight/combat as international terrorists
2	continued interest in mental health apps in lieu of mental health professionals
3	above average civil unrest caused by states changing their political parties
4	increasing disparities between urban and rural communities as the urban sprawl continues; inflames the division of how the military is seen by society;
5	armed forces behaving badly

Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	regulation of mental therapy apps	
2	senate pass campaign finance reform	
3	military work on the narrative of who we are and what we do in order to attract urban individuals, higher income individuals, etc. to serve within the force	
4		
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Need to prove that we can handle high-level political dissonance; can we learn something from how we recovered from Vietnam ... need to see that we can get out of this political era	
2	Our investments in recruiting new talent to serve and defend our country are so successful that we regain our military advantage in information warfare	
3		
4		
5		

Team Members:	**Purple Pawn 3**
Team Title:	**Purple Paws**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	solitary confinement of your media environment
Grouping 2	News desert: National news increased professional and decline of local news
Grouping 3	5G gives availability to push huge information
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	National Guard active duty soldier - intelligence officer with access to electronic communications
Where do they live?	Arizona native - Mexican American male 20 years old
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	Mexican government
What is the threat event?	Emergency situation at Arizona-Nogales border declared by US President/Mexican President allegedly due to cartel murders; false flag of Mexican government conducting ethnic cleansings in border towns on both sides in Arizona and framing Cartel for it; incitive event is a shooting of Border Patrol agents at border check 20 miles from AZ-Mexico border.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Martial law instituted in Mexico; US military brough in to enforce Mexican martial law
Who else in the person's life is involved?	Family is ranchers in the area on
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Mexican government want to seize territories back for Mexican posession.
What vulnerabilities does this expose?	US media and intelligence is blind to what is really happening at the border
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	A lack of open source info via the media due to lack of reporting and lack of cooperation at local level; and duplication of what is being fed by Mexican government/media. Therefore, President and military is deployed. In comes our protaganist Juan who is deployed to the border. All the algorthyms that intelligence community is analyzing including DHS - vast majority of data inputs are on Mexican intel side and are slanted as malinformation. This goes against what Juan's trusted network on the ground at the border is saying and reporting.
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	Spent military resources to eliminate Cartel on behalf of Mexican government for the Mexican government to take over drug trade in partners
Question One	Answer your question in the yellow box
What are the broader implications of a threat like this? What might a ripple effect look like?	Personal and governmental financial motivated gains; chaos; NAFTA trade threatened - new "Afghanistan" at the Southern border
Question Two	Answer your question in the yellow box
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	Media informed by malinformed (by Mexicans) intel. Social media (big tech) follows.

PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	Personal trusted network providing the reality check on what's being reported. US Intelligence community; Homeland Security; DEA
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?	Taliban looking for opiate markets
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question	
Question One	Answer your question in the yellow box
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	
Question Two	Answer your question in the yellow box
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)	
Examine the combination of both the Experience Questions as well as the Enabling Questions.	
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.	
1	
2	
3	
4	
5	
6	
What are the Flags?	
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?	
1	Mexican government behavior
2	Cartel behavior
3	
4	
5	
6	
7	
Milestones:	
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	Reconcerted effort by U.S. intel community to incorporate human sources to analysis
2	Legalize drugs in the US to dry up the market
3	Reduce dependence on automated analytics in the IC
4	establish grants to support local investigative journalism
5	legislate IP protections of articles to mandate attribution and citation, especially for articles that are simply reskinning of existing articles from need sources
6	allocate minimum levels of data collection from the field, to validate source inputs and to develop alternative sources
7	weigh information used to form findings to ensure outside perspectives are considered
	stress test data for likelihood
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?	
1	
2	
3	

Team Members:	**Black Pawn 3**
Team Title:	**Crismon Tide**
Estimated Date of the Threat:	**2029**
Data Points	
NOTE: Roll the Dice to pick a data point from each of the research areas in the Research Synthesis Workbook (the rollup for each "SME Grouping" or topic)	
Grouping 1	reflexive control
Grouping 2	Leaders describing divergent views as fake news
Grouping 3	Manipulation in augmented reality
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. Try to use the random inputs from the dice rolls above. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	
Who is your person and what is their broader community?	Captain Avery Victoria, US Navy Virginia Class Fast Attack Submarine Commander - graduated 1st in her class from Annapolis
Where do they live?	Yokosuka, Japan
Threat Actor or Adversary	
NOTE: Pick a Threat Actor or Adversary:	
1) State Sponsored	
2) Non-state Sponsored	
Put your Threat Actor or Adversary here:	Russia
What is the threat event?	Russia will create false tension in the region by spreading fake news and simultaneously manipulating US navy Senior arrays and on board maintenance systems.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	Increased Tension Between the USA/Russia and Japan. Capt. Victoria believes that she is defending the Japanese coast but she really sunk a Japanese naval vessel.
Who else in the person's life is involved?	US Govt Officials/ Japanese Govt Officials/her parents
What specifically does the Adversary or Threat Actor want to achieve? What is the Adversary or Threat Actor hoping for? What is the Adversary or Threat Actor frightened of?	Russia is seeking to decrease American presence in the Western Pacific. Russia is seeking to create tension between a newly independent Japan and the US Govt. The sinking of a Japanese vessel would compel the Japanese govt to ask the US military to decrease or abandon its military basing in that country. Additionally, Russia has been planting stories of atrocities committed by US military personnel throughout Japan. Capt Victoria is being manipulated by fake news of increased possibility of conflict between US/Russian. the Russians are micro targeting her through he social media profile and her fathers high position in the Federal Government. Russia has also determined that because of her strict upbringing she will follow orders despite any personal feelings she may have about not attacking a Russian ship.
What vulnerabilities does this expose?	The viability of fake news, the technical vulnerability of off the shelf products used extensively by the USN. Also the current tensions between traditional allies in the western Pacific Region. Increased use of AR to perform basic shipboard functions and Fire control
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two) from the drop down selections	
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
What will this make your person do that they normally would not?	
What is different and/or the same as previous events or instantiations of the threat?	
When the person first encounters the threat, what will they see? What will the scene feel like? What will they not see or understand until later?	
How will information be delivered to the person? Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)	
What will the person have to do to access people, services, technology and information they need?	
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	Answer your question in the yellow box
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	Heightened tensions across the Pacific Rim concerning US presence in the Region. Russians very vocal about America permanently leaving Japan.
Question Two	Answer your question in the yellow box

What will this make your person do that they normally would not?	Captain Avery orders attack on what appears to be a Russian war vessel in Japanese territorial waters. She actually sinks a Japanese coastal defense Ship.	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)		
Questions (pick two) from the drop down selections		
Instruction: Use dropdown to pick one question >>>>>>>>>>>>>>>>>>>		
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?		
New Practices: What new approaches will be used to bring about your threat and how will the Adversary or Threat Actor enlist the help of the broader community?		
Business Models: What new business models and practices will be in place to enable the threat? How is it funded?		
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?		
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?		
Russian/China/Iran/S. Korea (Big 4) culture/politics placeholder question		
Question One	Answer your question in the yellow box	
Barriers and Roadblocks: What are the existing barriers (local, governmental, political, defense, cultural, etc) that need to be overcome to bring about the threat? How do these barriers and roadblocks differ geographically?	Very few barriers exist today especially if a nation state applied resources today	
Question Two	Answer your question in the yellow box	
Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?	Existing technology systems today can prolieferate these types of attacks. Develop AR for DOD Armed Forces (Navy systems) for maintenance of critical weapons systems. Public and Private networks.	
PART FOUR– Backcasting - The Defenders (from the perspective of the defenders)		
Examine the combination of both the Experience Questions as well as the Enabling Questions.		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) ***do*** have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2029.		
1	DOD armed services ensure trusted supply chain in defense acquisitions (who is manufacturing the solution, where was it manufcatured, etc	
2	Develop and invest in technologies to identify Deep Fakes	
3		
4		
5		
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	Continued acceleration of innovation and technology	
2	Nation State investment and development of reflexive control techniques	
3		
4		
5		
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Unfortunately, nothing - many of the technologies and loop holes are available today.	
2		
3		
4		
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		
1	Continued investment in K-12 education (media literacy, critical thinking)	
2	Develop systems, and procedures to verifty and promulgate "ground truth" in crisis situations. In this sceanario, the US sank Japanese vessel, and everyone denies what happened - we need secure systems to validate and promulgate what actually took place, so that diplomatic entities have facts to negotiate solutions.	
3		
4		

Backcasting Workbooks

(Third Workshop)

G1B1		
Experience Title:	**Invisible Force**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	A battle for truth. Struggle to influence the information environment to our advantage. We can't control it, so how do we leverage it to our advantage while maintaining our American ideals, they are being used against us.	
What vulnerabilities does this expose?	The two ends of the spectrum, feedom and control. Adversaries leveraging our freedoms against us and then highlighting our controls as hyprcracies. Stating our controls violate our own principles. Is it freedom of speech if we deny access or sensor.	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	Have to have the capability to insert our narratives into any system, at any time	
2	Authorities to act, respond, and deploy information capabilities	
3	Government regulation of information dissemination platforms	
4	Analyze, monitor, and influence the private data of foreign national's data to de-legitimize adversarial information	
5	The ability to conduct CNA, CND, and CNE on adversarial controlled information infrastructure	Humans as sensors using police tactics as example. Legally they cannot collect, but they can sense. Sensing data is collected and analyzed. Sensing is dependent upon world view. It is effected by world view. How do you analyze sensing data riddled with bias... to make it actionable.
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	Development of AI/ML - unconstrained access to global data (authoritarian) - therefore, they have the time to start training effective AI now for use, 10 years from now	
2	We don't have control over words and concepts in cyberspace until people, societies, populations act on those worlds. However, our adversaries can	
3	Motivation for influence (OROB) - national debt due and consequences - implications, such as Venezuela	
4	A nation's partner of choice - China outspends us and Russia out arms - example China lends for infrastructure and then uses is own labor over local	
5	Space and there ability to control ground level perspective - counter space	
6	Expansive of the great fire wall to include nations they put information infrastructure into - expansion of social	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Highlight adversarial vulnerabilites through narrative - oppression of minorities, indebting of non-industrialized nations	National information agency,
2	Stop exasperating our own issues - producing narratives that disparage ourselves - poor job of mitigating our own issues	Whole nation

3	How do we need to train our soldiers for response to deep-fake at the tactical level; Cultural awareness; use the SOF models; focus on relevant training - 350-1 distraction; Field time - more time spent practicing our skill craft	TRADOC
4	Soldiers as technologically enhanced soldiers - cameras, recording devices to capture what occurring in the field	
5	We need to have the capability to identify the deep-fakes and state why its fake, how they created it; Social component - sell it to legitimate media sources - sources world views as reputable for truth telling	Army, DoD, USG
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Congress and senior leaders of the DoD to be willing to **accept more risk** - youth	Congress - DoD senior leade
2	Use of available data sets for training AI/ML algorithms - if we don't and our advesaries do, are placing ourselves at risk	Congress, DoD,
3	Counter space technologies - ability to protect our assets and defeat theirs	DoD, Space Command
4	More willing to use classified capabilities (cyber,space based) at the tactical level	Dod
5	Stop overclassifying capabilities - Snowden tools are within the open-source space; however, classification forbids us using these tools at the tactical level; our adversaries are using our own tax payer funded tools against us....	

G2B1		
Experience Title:	**Invisible Force**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	China has positioned itself to control and influence the economic, information and diplomatic environment in order to achieve desireable conditions without the use of overt military presence, specifically the ability to generate plausible narratives and target individuals	
What vulnerabilities does this expose?	Lack of priority given to there integratation of the physical, informational, and cognitive domains by failing to seize and retain the initiative.	
	Dual-use ICT systems manipulated by hostile actors, constraining friendly actions to affect that system.	
	Lack of diplomatic cadre, a reduced number of FSO, lack of global efforts	
	Lack of competing economic influence and ties within country	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	Risk aversion and authorities restrain the ability to execute IRCs. This must be addressed through policy and military culture.	
2	Difficulty and legal challenges to training in the IRCs; specifically EW, CO, MILDEC, CMO, and MISO. Address this concern through DOTMILPF and policy/regulation.	
3	Work to preclude and counter the distribution and employment of ICT from malicious actors. Offer competitive solutions developed by friendly nations.	
4	Diplomatic efforts to build up the image of UN/ Foreign forces prior to and during the deployment, build relations with population	
5	Maintain and increase interaction with host nation and local populace through various agencies and at multiple echelons of government.	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	No viable alternatives to Chinese owned ICT providers in Africa	
2	Evidence of successful low level deep fake attempts, integrated into the operating environment	
3	China or threat is able to gain economic control in host nation, with long term infastructre and assets	
4	As nondiscretionary spending requirements increase for the US, the DOD faces reductions in funding.	
5	Reduction in funding and manning for the DOS and other diplimatic engagement tools.	
6	Growth in pro- Chinese messaging in the local environment, IE observation of China shaping the environment	
7	Inroads made by a Chinese version of Russia Today	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	CPOE/EW in order to preapre to degrade, disrupt, or subvert dual-use ICT in the event of its weaponization.	
2	Indoctrinate Information Warfare into military training programs.	

3	Develop and promolgate counter deep fake tech and knowledge	industry/ Cybercom
4	Increase of diplomatic and economic participation in vulnerable host countries	State / private industry
5	Prepare and maintain guerilla forces with complementary information warfare cells and training.	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Traditional manuever warfare is executed suborinate to grand strategy narratives via cooridnated information warfare.	
2	Install either aligned or neutral networks in vulnerable host countries, via cheaper networks (google blimps)	Western Industry
3	Secure/Protected communications capability for soldier use to replace civilian technology dependence.	Google, SpaceX, etc
4	Establish and conduct sensitive Title-50 activities with sympathetic populations.	
5	US strategy should have Redlines, and actually defend them, enhance credibility	

G3B1		
Experience Title:	**Invisible Force**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	The adversary owns the inftrastucture and is the communications is across all domains, in both the operational environment as well as the homefont. Continual engagement with the information environment	
What vulnerabilities does this expose?	Reliance on 5G network for communication creates opportunities to exploit vulnerabilities and attack network credibility. If the Chinese and proxy forces are primarily using the communication network as an attack vector, the US can disrupt this and degrade their capability to message. Furthermore, degrading the network within the Chinese border and preventing internet access to their population could sow distrust with the Chinese government.	
	Exposes a tactic technique or procedure that that can be used by any entity. Vulnerability for China, because the US can do the same actions against China. US can fuel unrest and motivate the population to oppose the Communist party because of the flaws in the communist system	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	Provide an alternative invastrudture for developing country - US initiative but acccomplished by Industry	
2	Reward information savy and exceptional soldiers/officers	Services(Army, I
3	Find a way to bring the information environment into the training environment. If we see and practice, one can integrate and reward	Joint staff
4	Developing units to provide the information capability to units that are already overloaded with current tasks to become experts across the current domains	
5	Leader education and development	
6	Actions within communities of the Chinese to message to the US	
7	Create same offensive capability and use against adversary to deter future operations. Would not need to lie since adversary commits crimes/	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	China willing to use proxy forces /provide information to lethally attack US forces	
2	Global expansion of Chinese owned networks	
3	Reliance upon Chinese owned networks by 2nd/3rd world countries	
4	Early creations of deep fake content	
5	How does China deal with current "information warfare"- i.e. Hong Kong. This will indicate future techniques, tactics, and procedures	
6		
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Understand how to exploit the Chinese/adversary networks	
2	Professionalize an 'information domain' force. This could be a top-down process or bottom-up development.	

3	Capability overlap- information maneuvar does not belong to just one unit. All maneuvar units deal with information warfare from infantry to cyber to SOF, etc.	
4	Military/Industry collaboration to innovate new concepts/technology to counter the threat	
5	Cultural/organizational changes to recruit the best fit persons to fill cyber/information jobs. Can the military take advantage of a "privatized cyber/information army"	
6	Exploit population grievances within the Chinese population	
7	Continue to respond to humanitarian crisis in order to establish and maintain US credibility. This will sway populations in the US favor when they must decide between a US narrative vs. an adversary's narrative	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Gain access to Chinese built networks both inside China and inside Chinese-supported nations.	
2	Need to develop our brand, and one that will sell itself and assure that the US/Allies are the best offer for mankind, not just the US	
3	Inoculate the population and education them against the issues in the Information Age.	
4	Educate the population on real vs fake- institutionalize critical thinking	
5	Education on the understanding of the new invastion. The economic invasion of the world by Chinese	
6	Develop a "encryted tag" to media to prove validity of digital media. Tags will be given to 'vetted' reporters. This will help diminish the credibility of deep fake media that is injected into social media (if it is missing a tag).	

G4B1		
Experience Title:	**Invisible Force**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	China has had the ability to get proactive in operating enviorment vs our reactionary response.	
What vulnerabilities does this expose?	The chinese capabiltity to conduct reflexive control and US lack of capability/willingness to employ reflexive control at the unit level. The sheer number of people china can throw at a problem vs us capability.	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	BCT capability to monitor digital pattern of life in local area (In the S2)	
2	Culture change within the combat fighting force to see information maneuver as a critical piece of maneuver	
3	Resource control over rare earths, raw materials.	
4	Can American government influence media companies creating narratives that are contrary to american interests or supporting chinese narratives	
5	Chinese financial influence in American institutions	
6	Anti-Chinese messaging by American media institutions	
7	Domestic messaging tied to actual socio economic status to improve under served American regions to stimulate support for foreign partner investments	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	foreign digital reliance on chinese networks	
2	chinese control over natural resources; population information control	
3	Sino-African future population due to population interbreeding- where is the loyalty	
4	Black market that operates outside of chinese social credit system- what does this look like - is it digitally segregated or analog?	
5	Chinese whole of nation approach vs US separation between political and economic agencies/institutions	
6	Chinese force projection capabilties - what is their force presence/capabiltities outside of mainland china	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Whole of government approach identifying China as primary adversary on DIME and policies that support local infrastructure	
2	Forward deploy US forces to develop strategic partnerships across Africa (establish an infratructure foothold that enables information foothold)	
3	Establish gov't investment in food and water security (desalinization) that enables local governance and self sustainment/energy in Africa to build local trust to counter the information narrative	
4		

5	Develop capability and capacity to conduct "information maneuver" tactically.	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Phase AFRICOM to be physically located in Africa	
2	Develop military/economic/information relationships with African Union	
3	Target mass entertainment media environment to leverage emerging African entertainment/consumer markets	
4	Long term resource security focused on self actualization/self determining to avoid colonialism associations	
5		

G1B2		
Experience Title:	**Across a Dark Chasm**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	Wedging - creating conflict between groups working in solidarity	
What vulnerabilities does this expose?	The ability for adversaries to manipulate or create conflict from culturally different groups through virtual manipulation	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	Regulation, policy, law, and strategy that enhances the positive uses of technologies and diminishes its negative effects	
2	The acquisition and use of technology to include foreign national data - AI/ML training	
3	The ability to monitor and analyze data flowing across USG networks and devices; control military members use of personal IoT devices	
4	Ability to access, exploit, or attack adversarial controlled networks within the cyber domain	
5	Conduct physical engagements with allies and partnered groups as a method of validation	
6	Public service announcements that raises awareness of these possibilities	
7	Acquisition of technologies and where those technologies are manufactured	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	Allies and strategic partners networks, network devices, or the controls they emplace for the use of these technologies	
2	Unethical use of technologies in novel ways; troll farms, deep fake content production (disinformation)	
3	Adversary network, network devices, or the controls they emplace for the use of these technologies;	
4	Service member's family's network, network devices, or private data	
5	The creation and managment of foreign social media applications	
6		
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Acquire data set necessary for training AI/ML to identify and learn recognizable patterns of social media manipulation	
2	Create incentives for companies/corporations to manufacture networked technologies within U.S. regulations for these devices. To include the mining of the semi-precious metals used to create these devices (anti-hardware hacking).	
3	Increase the protection of intellectual property and the regulation of the devices used by service members abroad	

4	Educate service member's family on the necessity of validating information acquired through social media, solely dedicated to the families of deployed service members. Establish a Military contact agency dedicated to validating this information.	
5	Establish physical engagement and validation protocols as a response measure to reported incidents of social media manipulation affecting strategic partner relationships.	
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Develop an AI-driven persistent virtual force that monitors for patterns of social media manipulation; learns of adaptive techniques; and identifies sources of social media manipulation	Whole of governr
2	Include the necessity of coalition social media manipulation task forces within Status of Forces Agreements	State Dept., Dod
3		
4		
5		

G2B2		
Experience Title:	**Across a Dark Chasm**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	Adversary has broad based persistence access to information presented to the military in both official and unofficial means in order to create weaknesses between forces	
What vulnerabilities does this expose?	Cultural manipulation, by exploiting views on privacy	
	Attack vectors are small of in scale and impact not an immediate threat, but culminating effect could achieve a major effect	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	Promulgation of Information enviornment conditions and standards to report abnormalities	
2	Build positive enviornment through IO campaign on own forces.	
3	Planning and encouraging social engagement	
4	Real time analysis of our own social media footprint	
5	Map and analyze military members who are vulnerable to manipulation or exploitation - OPM, Posts	
6		
7		
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	Abnormal cell and social media behavior	
2	Insider threat behavior	
3	Adversary media outlets developing narrative counter to reality, supporting their IO campaign	
4		
5		
6		
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Integrate a WEB Opsec cell into the Corps' I2CEWS/ Information Warfare Capability in order to provide continuous protection	Regionally Aligne
2	Monitoring or Fraud system for social media	Industry
3	Legal authorities to protect and defend all information pertinent to military objectives to inlude private social media interaction by active service members	congress
4	Enforce human interaction	DOD/DOS
5	Conduct intrusive IW campaign against adversary, use messageing against and take down capability	DOD, CYBERCO

What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Modelling of manipulation for own force, continual measurement of vulnerability	OPM, FBI, DOD
2	Monitoring and protection for SM family social media footprint	
3	Maintain IO training	
4	Maintain deterrent IW Campaign, to keep adversary on edge	
5		

G3B2		
Experience Title:	**Across a Dark Chasm**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	INDIVUALIZED personally attacks through personal network devices as well as AR/VR training devices as a micro deception effort.	
What vulnerabilities does this expose?	Risk for exploiting personal vulnerabilites exposed thorugh individual networked devices	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	Acquisitions process to develop network devices- built in resiliency and encryption to deter attack- hardware and software	
2	Education & innoculation of Soldiers and their families to current adversary TTPs throughout competition- we operate in a disinformation environment	
3	Improve "Virtual" integration with partners and develop TTPs and lesson's learned early and often. Maintain personal relationships to defeat an adversary's virtually implanted disruptions	
4		
5	Enhance people's capability to build personal trust through physical interaction. Enhanced social skills to build trust	
6	Work with social media and media platforms to improve authentification and security of current commerical platforms that Soldier's use	
7	PRepare to use same methods to attack the adversay and demonstrate our capability. Punish them for their actions by doing the same as a way to deter future attacks	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	Ability of Natural Language Processing to map to regional and cultural dialects. Elimination of cultural clues and errors in speech.	
2	Increase of non-discriminate targeting of families / soldiers	
3	Increase of discriminate targeting of families / soldiers	
4	Increase of adversarial deception operations through social media and tech applications	
5		
6	Adversary's collect and attack units and leaders at the tactical level (Interest by adversaries at lower level of org chart)	
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Develop resilient tech	
2	Educate forces and families	
3	Build pretected family/military social media network within an established framework (Facebook with a .fam. mil access only) that is firewalled off	

4	Government/Industry collaboration to protect privacy	
5		
What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	AI development to collect information on open-source platfroms to build org charts / order of battle to understand who potential individual targets are	
2	Artificial Intelligence Units that manage the entire environment to assist in the truth	
3	Win the AI "space race"	
4		
5		

G4B2		
Experience Title:	**Across a Dark Chasm**	
Estimated Date:	2030	
PART ONE: Threat Overview		
Describe the Threat Future as you see it.	Micro targeting of the persuadables and using old school targeting techniques in a new avenue attack	
What vulnerabilities does this expose?	we're more vulnerable to cold war tactics of reflexive control that are faster and more interconnected than under the cold war. the inabilty to agree that the russians are our enemies enables their continued freedom of maneuver. The adversary has the ability to get inside of our social decision making cycle.	
PART TWO – Backcasting - The Defenders (from the perspective of the defenders)		
Explore what needs to happen to disrupt, mitigate, and recover from the threat in the future.		
What are the Gates?		
List out what the Defenders (U.S Military, U.S. Government, Allies, Local and International Law Enforcement, etc.) do have control over to use to disrupt, mitigate and recover from the threat. These are things that will occur along the path from today to 2030.		
1	limit advertising/targeting data gathering on military, government, and family members	
2	develop and use bot networks to create defensive social media networks	
3	continuous media messaging to increase the awareness of the force and their families of dis/misinformation	
4	what are the limits of surveilance capitalism and what are the limits of what companies can do with this?	
5	Long term conditioning of digital skeptiscm within population	
6	periodic assessments of social relationships with partner nations forces (METT-C dependent)	
7	actions to identify vulnerable members of the population	
8	identify national loyalty that may be higher among immigrant pop vs native born	
What are the Flags?		
List out what the Defenders ***don't*** have control over to disrupt, mitigate and recover from the threat. These things should have a significant effect on the futures that have been modeled. These are things we should be watching out for as heralds of the future to come. What are the incremental steps to stated adversarial strategies? What are technological/scientific advances that could be repurposed?		
1	we can't control what social media people are on	
2	what are the free speech limits that the government can impose on media/data companies?	
3	Legal/regulatory limitations on data operations within US/targeted to US Citizens	
4	by ignoring lack of shared understanding of virtues and vices	
5		
6		
Milestones:		
What needs to happen in the next 4 years (2019-2023) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1	Messaging and Deterence actions through cyber means to known cyber threats	
2	AFN messaging on Russian Infuence Operations	
3	Improved IA training to discuss threats in Social Media and adversarial influence operations	
4		
5		

What needs to happen in the next 8 years (2019-2027) to disrupt, mitigate and prepare for recovery from the threat in your future? What are our actionable objectives? How should we use IM (Information Manuever) to accomplish these actions?		WHO
1		
2		
3		
4		
5		

Research Synthesis Workbooks

(Third Workshop)

	Group 1 Threat 1			
#	**Data Point**	**Implication**	**Positive or Negative?**	**What should we do?**
1	Reaction as a second and third order effect	Lose tactical patience, react before things play - importance of doing nothing - however, causes losing control. Loss of legitimacy within local population. Understanding the only way to control situation is to destroy it.	postive and negative	
2	Creation of legitimacy, local perceptions	Multiple U.S. agencies involved, ground presence, MISO team presence - dependent on local legitimacy	positve	Multiple U.S. agencies involved, ground presence, MISO team presence. How do we leverage tradional media or the social media sources (sources local population view as legitimate) to concur with our truths? Are there going to be Cyber teams/IW teams to shut down deep fake sources. Agencies dedicated to the dissemination of truths - who are the truth bearers? Is it a neutral third party organization the local and world community view as legitimate?
3	The truth cannot come from us, it must come from information sources considered legitimate/independent			Denial of access -
4	Denial of access to disseminate information	Speed and adaptability of threat create need for flexing offensive capability.		
5	Exposure of capabilities - tipping our hand			
6				
7				
8				
9				
10				

	Group 2 Threat 1			
#	**Data Point**	**Implication**	**Positive or Negative?**	**What should we do?**
1	Deep fake production	Adversary able to control the narrative	Negative, we have to prove a narrative, acknowledgement even gives creedance,	Potentially, ignore the message, WOrk with host nation govt, monitoring of social media, Use of Combat Camera to counter narrative or provide your own
2	Economic situation in country	Susceptibility to malicious actors	Both, pemrissive for both freindly and adversary manipulation.	Incentivize finance and investment in countries to provide option to Chinese investment
3	No skepticism in local population	Confirmation bias, population in cognative position	Negative, we would have to overcome and change it	Proactive from the beginning of the mission, Need to support a poitive, use of Public Affairs working with host nation
4	Reliance on Adversary network for comms in country	Provides access to adversary of our information, locations and provide targeting information	both, If we are in the network then be able gain reverse access.	SIgnature control, cell phones not allowed on mission, if cell comms required use a controlled device and network, OPSEC for entire
5	Chinese Adversarial Narratives	Vulnerable populations are proactively identified and targeted by the adversary.	Both, while competitors exist in this space BLUFOR should be operating in thise space oncurrently.	Integrated non-lethal fires for the operation such as introduction of forces, with branch and sequel narratives in response to changes in the IE.
6	Threat knowledge of Friendly Forces personnel	Lack of operational security allows threat to determine extensive information about personnel in UN force. This allows them to generate targeted disruption tools with high impact. Essentially spear fishing with psychological operations	Negative, allows both tactical targetting and long term disruption to morale/ loss of trust	
7				
8				
9				
10				
				Integrated non-lethal fires for the operationg to include introduction of forces, and branch and sequl narratives in response the the IE.

	Group 3 Threat 1			
#	**Data Point**	**Implication**	**Positive or Negative?**	**What should we do?**
1	Deep Fake video of Soldiers and operational actions produced by adversary	Narrative mobilizes local population to act agressively against the US base	Negative	Establish a robust narrative in anticipation of this event. Messaging needs to be built prior to event and ready for employment. The issue becomes the number of tactical narratives is infinite- how do you prepare a counter-narrative for a specific event (deep fake of raping women) without knowing all the potential scenarios. Strategic counter-narratives are 'simpler' because you can target an ideology vs targeting a specific event.
2	Targeting of Officer by phone	Concern over the home front can target Soldiers forward	Negataive	Need to protect not just the forward Soldiers and the families in the rear
3	Deep Fake Videos	Rapid, credible messaging influences global populations	Both	Fight narrative both by destroying the credibility of enemy propaganda while also promoting a postive message of US successes that counter the enemy message
4	Multiple communities engaged	The public affair messaging in the rear is crutical as well as in the theater.	Both	Media engagement plan that is coordinated from the front to the rear.
5	5G network controlled by the Chinese	Freedom of communication and networking	Negative	Attempt to exploit vulnerabilities within the network
6	Disengagement does not stop spreading the message	Just not being in or on the network can not prevent the targeting of families in the rear	Negative	How can we engage with the network of families and supporters in the rear area.
7	Chinese willing to facilitate lethal action against US	Chinese Government is willing to take more risk towards escalation to lethal conflict	Negative	Make China aware the US recognize China's action, and it is escalatory, The US would be willing to escalate to match Chinese actions. USe same TTP to cause Social unrest in China.
8	Social Media Influence / Messaging	Direct 'personal' influence	Both	Restrict use of personal devices?
9				
10				

	Group 4 Threat 4				
#	Data Point	Implication	Positive or Negative?	What should we do?	
1	why was the video believed/mulitple supporting evidence	social media support for narrative, video itself,			
2	chinese network control	message propagation, institutional support, institutional ties, financial ties, colonialism w/o colonialism narrative			
3	information security/dual use technology/reliance on civilian communication networks	digital signature gave legitimacy to the video			
4	no UN/West counter evidence or alternate reality pres	Friendly force must actively present information in support of their interests	These vectors/capabilities present both opportunity and vulnerability	Actively present information in support of operations	
5	why did this video spread?	influencers on the ground, what is government's role, how does tech enable propagation		can we leverage local personal relationships tied to formal and informal power brokers	
6	no traffic monitoring capabilties	what monitoring capabilities can we use to see uptick in chatter,	opportunity and vulnerability	technologies to monitor real social growth of an idea vs algorithmicly driven traffic boost	BCT capability to monitor digital pattern of life in local area (In the S2)
7	comms asymmetry between the brigade and the adversary; terrestrial, space based, organic v. national	The brigade is not equipped with organic equipment to mass information as the adversary is	negative; but how does the brigade leverage slow, accurate information	is there a way to leverage slow information for verification vs speed	
8	BCT training focus on full spectrum operations which means the training environment is focused on combat vs engagement with noncombatants	military decision makers are not being trained to leverage information environment/cyber/virtual		need operationally relevant training in a representative environment (realistic training with civilians not just blowing things up)	
9	Lack of information warfare focused on US civilian messaging	information operations overseas vs information warfare - we can't keep ignoring the civilian message factor			
10					

	Group 1 Threat 2			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Losing the gap between human-computer interaction	Erodes reality - inside the social media makes it easier - more postive - makes us more insensitive - digitization masks the consequences of actions	Negative and positive	sensitivity training? how do we maximize while mitigating the cognitive implications?
2	Subtle virtual deceptive changes that influence how consumers of the content think	Sow dissent against allies and partners; subtle changes are more effective at changing minds than information overflow - long term effects are powerful	Negative and positive	Recognize them and address them
3	Virtual scripting that defies belief	paralysis - failure to act versus over reacting	negative and positive	redundancy in validating information - multiple check
4	Manipulated meetings between groups in conflict - taking advantage of an existing problem by bringing them together	drive wedges between unified groups - deteriorates the strength of solidarity	negative	pattern recognition - add layers of validation for identification - information assurance within the social media space - anonymity is a danger
5	Micro targeting and the creation of conflict - fabricating reasons for individuals and groups to dislike or be in conflict with one another	sow discord, polarization, civil war - destroy alliances and traditional organizations	postive and negative	Trust and authentication on social media devices; regulated; physical instead of virtual engagements
6				
7				
8				
9				
10				

	Group 2 Threat 2			
#	**Data Point**	**Implication**	**Positive or Negative?**	**What should we do?**
1	Active Information campaign	No matter the format, VR, Social Media, adversary has access to manipulate	negative	enhance face to face contact, promulgate understanding of disinformation environment
2	Control and Defense of data	What is the legal definition of data	Both, potential for police state, monitored state	balance needs to be strucked
3	Targeting individual relationships	Able to find a speific thread in which to exploit	Positive, enforce the goal of interpersonnel development	Maintain interpersonal contact, screening social media activity
4	Sensor to detect modifications in social media	massive data stream and collection,	Both, potential for police state, monitored state	Fraud alert on data streams
5	If I can target you for military effect against your 'personal' life, is it still personal?	That during military action, you are continually on duty and all aspects of life are controlled/monitored and collected	negative no true privacy, positive is that there is protection	military control of all aspects of life Condition SM's to understand intrusions
6	Russian fixation on Vices	opportunity to highlight their preoccupation with "deviant" behavior, turn the negatives against them	Both	Have allies participate in counter narrative, exposing their efforts
7				
8				
9				
10				
		If I can target you for military effect against your 'personal' life, is it still personal?		

	Group 3 Threat 2			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Virtual Reality Training Environment that is exploitable	The advanced and indivualized traininging provides a new attack surface with individual effect.	Both	Ensure that we have security and overwatch of training and ability to review training to see about motification
2	Trust between individuals becomes a target	Degrading of trust in confidence of personnel in a unit or coalition	negative	Units and coalitions need to build more resilience in terms of trust
3	Targeting of family members	Brings the network into play and the targeted attack on the Soldier into a targeted attack on his family.	Negative	Need to find a way to secure out families and networks.
4	Access to the individuals and can portray individually	Every soldier has personal vulnerabilties that an adversary can blackmail for effects	Negative	Protect personal data
5	Just reducing the effectiveness of the unit is a high impact low cost attack. The cost is the AI/Research ML, and then the attacks cause discontent for free	Information domain because a part of readiness	Both	Education of the force to understand the effect of targetting
6	Personal turmoil	reduce overall unit and combat effectiveness	Negative	Protection of Soldiers from personal attacks
7				
8	Relationship between US and Polish partner was not strong enough to identify false information . False information was festering instead of being addressed and discredited earlier	Units, Families, Coalition Partners must have resilience and inoculate against fake news and false narratives prior to attacks. When something odd is sent or seen, forcing people to question it before believing it.	Positive	Find ways to educate families, soldiers, partners on the possibility for fake news and false information to spread.
9	Units and Leaders do not have visibility on the media and communications going to soldiers	This is an attack surface that needs to be considered by leaders.	Negative	Consider how soldiers and families are affected and prepare for it
10	Adversary wants to create discord within units and partners	creates an opportunity to employ deception by providing the enemy what they are looking for	positive	Units should ID attacks and feed Russians what they want to see. Units will ignore attacks but Russians believe they are being effective.
11				

	Group 4 Threat 2			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	lack of information warfare innoculation	more effective information assurance training		mandated training - build skepticism and trust into the force
2	technology integrity/supply chain protection and assurance			we can't monitor everyone's social media but can we monitor what they're exposed to with advertising?
3	fall out from fighting the local nationals that highlight the lack of support for locals and military	Eroding trust at the local level while elites say the relationships should be trusted		routine drinking and socializing between local and military folks to build social cohesion
4	Social engineering attack vector that resulted in compromised individuals: who are the persuadables within the formation	can we do an intelligence prep of our own forces to identify these vulnerabilities that the enemy might be able to exploit	opportunity and weakness	better systems to identify social weaknesses and strengthen these avenues of attack
5	who are the persuadables within the formation	how do we identify when someone has been compromised		how to we innoculate the force against mis/disinformation
6				
7				
8				
9				
10				

Post Analysis Workbooks

(Second Workshop)

	Round	Team	Round One - "Summary"
	1	Red Pawn	young mother, 1st nations community, rural community, Pad, artist - Bailey - born 2009; Paducah, KY - 3rd most prominent micropolitan// shipping transport - Walmart; Chinese multinational wants to interdite; Chinese multinational creatres social media narratives - recycled memes, old stories about shabby product, underpayment of workers - first native american, then other subgroups, including the head of logistics, use AI autogenerated communities of fake workers complaining. emails and messages are interdited with a phishing attack disguised as a link to the AI genreated Audio/video deep fake "exposee" videos - to secure logisitcs/operations credentials - also bots targets workers and employees - her customer data handsets have unique explicit user profiles/shopper history; friends, coworkers, tribal members and customers; actors intent is grwoth and market share, looking to create a dependancy on their network and services - short term goal is interdicting Walmart, long term goal is capturing logistics inventory/port
	1	Orange Pawn	Joe Snuffy - social media influencer at a univeristy; Low econmic community in the suburbs of st. louis; Deep Faked podcasts using his voice, similar enough to his topics the make it impossible to deny; People are questioning his new views, peers disassoiate, univiersity questions motives. Starts panicing; close family, significant others; they want to use the legitamacy of the podcast to disseminate their message; Vulnerabilities: truth verification
	1	Yellow Pawn	Akito Naruhito, decendent of emperor Naruhito of Japan; Climate change is influencing Japanese strategic decisions to consider new territory to enable national/cultural surivival; Akito is a target of Chinese IW trying to divide her (as an influential political and military symbol) away from achieving Japan's "first boots on land" strategy in China; Akito is the daughter of the throne reestablishing the Empire and dominance of Japanese culture through the pacific. She's responsible for establishing the resurgent warrior culture in Japanese culture; Akito's daughter is 7, and has grown up in a hyper-connected world and is POINT OF vulnerability for digital exploitation. Compromising deep fakes of her daughter in sex has caused Akito to rethink the Japanese strategy to retake population/territory. She is now focused on finding the perpetrators who are attacking her daughter/ family honor; Japan is
*	1	Teal Pawn	Middle School Civics teacher; Mrs. Foley; older gal that remembers how democracy used to work in the early 2000s; Iowa; Refugee camp as there is only 1 farmer left in the area; Mrs Foley gets targeted to purchase textbooks that are re-writing history as anti-democratic party is changing society; influenced to burn old textbooks that might "correctly" describe history; in the future everyone's textbooks are personalized and open to the highest
	1	Purple Pawn	Corporations + Information tribes/ Haves Have nots due to infrastructure access; Urban/suburban/virtual = first world of US; rural, poor access; reservation = third world of US; Huge divide between tribes and urban vs. rural; Experience life as a non-citizen, cannot participate in society (politically, economically, socially, knowledge) fully ; Want to achieve information dominance - they are the controllers and governance of all information for purpose
	1	Black Pawn	Kai Foo Lee CEO and evil mastermind ; No country of residence - lives everywhere and lives nowhere (currently residing in Four Seasons Suite in Hong Kong) along with his 44 well armed security detail and 500 data scientists.; Cornered the majority of AI/ML technology; controls education systems and hiring practices of all technology companies worldwide through his algorthmtic approach to everythingKai Foo Lee's love of life was misdiagnosed due to a fault AI/ML algorthrym in the US Healthcare system and lost her life as well as her unborn twin boys Several unknown mistresses and his daughter
*	2	Red Pawn	Bobby Jo, female flight attendant, visiting Athens Greece, 28 yr old, from Atlanta, based in NYC, the business class attendant for the Atlanta to Athens run, has friends and relatives globallyfrom Atlanta, based in NYC; North Korea, state sponsor by proxy, to a Russian private bio tech company in Chinese crypto currencyfast mutating bio bomb launched at an airport hub for max distribution to global transit hubs - our flight attendent is patient zero, but the bioweapon is programmed to show know signs. She is our Typhoid Mary. "kill democracy where it began"; While in Athens, she is posting to instagram, she has a simple wifi spoof, her mobile device, and her biometric info ID is hacked. That contains her bio info security access. This is used to develop the weapon that turns her into the carrier - but shes carrying a digital virus in her biochip/augmentation. It is used to infect security personnel. Using her data to access airport systems, best infection vectors are pulled from security lines for enhanced inspection, propogating virus from security to civilians at scale. Targets the airport security system to manipulate the secure search; infect a fast moving virus to the TSA/security person; weapon is genetically bifenced to US citizens in FDA database, goal to unify Korea with North Korea at the head, and eliminating US resistance and removing them from global stage; Vulnerabilities: we have a bio chip enabled population with biodata for all citizens; the implanted augments that create positive effects (deeper movie experiences, etc.) are virus factories waiting to be tripped; second phase of hack is psyops using the original Instagram account hack to deploy algorythims across social nets to (a) scrub mentions of the symptoms such that there is lower awareness of the disease and (b) create misinformation narratives about infected or uninfected demographics to drive blame, division and violence (e.g, 2030 census takers, dems or repubs, muslims, etc.); first encounter at a popular bar/cafe in Athens, and completely oblivious to the exploit. they'll not realize their digital exhaust was used to target them, that both their social and bio info were compromised, that the virus was custom-built to show no signs in her, but to fast mutate to avoid detection, and that digital feeds wont let info spread; Broader implications: Coordinated mal/misdisinformation attack means virus spreads faster than truth: virus fans hate, differently affected groups feeds into multiple hate-based narratives ("well only dems are getting this") bio attack disables traditional medial forensics; secondary consequence is wealthy elite wiped out, surivivors are people opted or unable to be chipped (undocumentned immigrants survive); Barriers/Roadblocks: spoofable wifi or connectivity; biochipped population and a centralized databaseet; portable bioengineering devices; airports and key facilities using genetic and bio markers for ID; hiding activity from US cyber intrusion; relative genetic science; Ecosystem Support: Chinese Cryptocurrency, Russian Biotech; North Korean ransomware money; academic research funding; Gates: established intelligence network monitoring adversary networks, quantum encryption to defend biodata, redundant security agencies in major transport hubs, quarantine, securitized IOT/global protocols; Flags: portable genetic engineering tools to splice custom engineered viruses, implanted augments that translate digital info capable of generating physical/psychological effects, IOT hubs at the Edge/ Global IOT protocols, academic/medical research freedom/sharing of research info in non-security communities, freedom of movement/ global quarantining; Milestones (4 years): Enhanced security authentication protocols in addition to biometric, regulate the write privileges of the bio chip (specifics on what can and cannot be coded), Global IoT Protocol, An effective World Health Organization mediated Treatise, Explore globally banning and penalizing bio-devices that produce physcological effect devices, Credentialing of IoT information sources (accredited media) to counter dis, mis, and malinformation; Milestones (8 years): Hardened augmentation... what is added to your body. Trust, how do we trust these devices? If we can be hit with a bio weapon, such as a sound weapon, then I can hack you from a distance to hack bio devices (the augments), Develop technologies to update and patch the force's augmented (bio) devices from credentialed sources; rapidlyDevelop AI/ML algorithms that analyze and identify anomalies/patterns within open source information indicating the creation and use of bio weapons that attack bio implanted devices, Create a system that protects research institutions IPs; create a framework for institutions to securely share research information; digital camouflage (can't see you, then they cannot hack you concept), Develop a tool capable of recognizing modified DNA or genetic modification; example TSA scanner
	2	Orange Pawn	Joe Snuffy, Rural farmer, Citizens of rurual communities from Taylor, Arizona; Offers from state actors in Mexico creating allies with Southwestern Farmers to potentially secedeMexico with Chinese/Russian help. The United States has been successfully countering Russian and Chinese information operations with AI and better cyber tools. However, since the completion of the wall, Mexico now sees the US as an adversary and the Russians/Chinese see an opening with Mexico as a proxy to get tanglible results from an IO. The growing secession movement in the US Southwest is seen as the perfect storm to break up the US by the three adversaries Secession actions are local issues and these Local issues not making up into current ploitical enviroment/discussionSince 2019, Mr. Snuffy has been disenfranchised, political matters that are important the rural communities dont make it to national platforms. This is futher exacerbated by removal of electoral college and a recent push to increase senate to represent more populous
	2	Yellow Pawn	Carmine Santino, son of one of the 5 families; age 20, supervises logistics systems at the docks in Newark, New Jersey; District Attorney is running a campaign against the Santino family, wanting to reign in corruption; doesn't understand the connections that the mob controls; using AI to generate the entire video content; Young & idealistic DA plus a very public push for "Goober" (Uber for sustainable trash pickup) is a sensational idea generating lots of campaign money for public officers who support it.Deep fake video shows his father at fund raising dinner and links to other phones at the same event showing the same video talking about screwing over the sanitation workers; threat is that by taking down the crime family interupts sanitation/garbage collection,Carmine has to figure out how to counter the deep fake video IOT reassert his Family's control over the garbage industry without causing shame, without doing something (too) illegal, and needs to prepare for the next wave of smear the DA's office is about to releaseCarmine's cousin Sylvia is a computer science student at Columbia U, interning at New Jersey DA for a semester. She tips him off that the DA is prepping a larger smear campaign than this first video. Sylvia got her internship because of an AI-enabled search that selected her from 100,000 candidates of computer science students in the greater NYC metro area, based on analysis of her public and semi-public ("data exhaust") profiles AND a requirement to select diverse candidates. DA wants to undercut the influence of the Santino family as part of the office's fight against corruption and mob control over economics; Vulnerabilities: how unseen/ignored actors influence daily life; this is an example of "reflexive control" meaning forcing the son (Carmine) to act in a way favorable for the DA is a way to control the father and the Family.; He will have to reveal his capabilities to access the internet and spoof biometic data that are outside of the legal means of accessing the internet; Even though Carmine approached his dad to confirm the video was fake (because no one trusts videos anymore), his father told him not to take any illegal action (hacking). Impulsive teenagers/young-20s want to show how he protects the Family.; Difference: to counter this, he will have to hack all the original gadgets the state drew on to develop the AI fake and push the unaltered video; New threat practices: Internet use/ commerce/credit system is tied to biometric data; burner phones illegal; highly connected devices are vulnerable to AI attacks to turn on multiple devices in a particular area, capture video/audio, and re-create an AI-generated environment for DEEP, deep fakes; Barriers/Roadblocks: Data privacy law has taken effect which has then subsequently reduced anonymity of data. The legal environment has taken away civil liberties that makes government surveilance of individuals devices easier by tying internet enabled devices tied to biometric markers. The Supreme Court has reinterpreted privacy to individual not their devices or data. ; Gates: Loyalty - controls clean sanitation services for the cities which builds good rep with citizens; Coming/going of people within trust circles in the family; they can choose who is put in certain areas; Need to have access to secure tech that bypasses requirement to tie personal IDs to devices (i.e. biometric spoofing or anonymity tools - probably illegal now); Flags: DA in enforcing the law, has to go against public opinion and upset the Family's good rep with citizens; Privatizing of public services such as "Goober" (Uber for sustainable and eco-friendly trash pickup); Speed of AI technology - dual use; Amount of garbage mob's trash system was picking up is being reduced by environmental impact measures and improvements (i.e. back to highly recyclable containers, which feed the demand for 3D printing raw materials); Milestones (4 years): Rapid development in recycling advancements - repurposable recyclables, esp. for 3D printing; Rapid improvements in AI that can create entire environments out of scratch, rather than deep faking a face over another actor in an existing video; Robots capable of separating old electronics increase the profit margin for recycling tech; Milestones (8 years): National data protection law passed (i.e. pseudo-GDPR) that also requires individuals to be tied to their devices - anonymity reduced; Children's biometric/DNA data can't be legally collected until they are 16. Kids are finding ways to get online without this DNA verification. Tech is secretly developed to support the illicit anonymity market.

	Round	Team	Round One - "Summary" (Ali)	initial themes
	1	Red Pawn	A young mother in the first nations community works in shipping transport at her local Walmart in Paducah, KY - the 3rd most prominent micropolitan area in the US. A Chinese multinational company wants to capture marketshare in the US via the largest retailer network. Their first goal is to create a dependency on their own network by interrupting and rerouting all Walmart empoyee data and systems traffic. They create social media narratives - recycled memes, old stories about shabby product, underpayment of workers, AI autogenerated communities of fake workers complaining - in first the native american, then other subgroups, including the head of logistics, to sow seeds of doubt and unrest across Walmart employees. Second stage of the attack includes phishing emails and messages disguised as a link to the AI generated Audio/video deep fake "exposee" videos	system vulnerability targeting, microtargeting, primary targets / secondary markets, private lives / professional impact (private professional blend),
	1	Orange Pawn	Joe Snuffy, a social media influencer at a University, living in a low economic suburb of St. Louis. An extremist/hactivist group is looking to disseminate their message and target him as a catalyst for dissemination, leveraging the legitimacy of his podcast and extensive following. Hactivists create deepfakes of Joe's podcast, recreating his voice perfectly, and swaying his subject matter just enough to continue to capture his regular audience with their own targeted message. Listeners begin questioning his views, peers disassociate, the university questions his motives causing panic.	mid-fluencers (medium-fame influencers) as platforms, exploiting normalcy, make it and break it
	1	Yellow Pawn	Akito is the daughter of the Japanese Emipirical throne reestablishing the Empire and dominance of Japanese culture through the Pacific. She's responsible for establishing the resurgent warrior culture in Japanese culture. Japan is mobilizing their community to regain their regional dominance that they had prior to WWII. As climate change impacts their landmass, they are looking for new territory to preserve the cultural /genetic empire. Akito is a target of Chinese IW trying to divide her (as an influential political and military symbol) away from achieving Japan's "first boots on land" strategy. Finding deepfake videos of her 7 year old daughter in compromising sex acts. Akito is forced to reprioritize her actions toward finding the perpetrator having	microtargeting, private lives / professional impact, cultural exploitation, emotional hacking
*	1	Teal Pawn	Mrs. Foley is a middle school civics teacher in Iowa. As urban populations increase nation-wide, rural communities have less influence on democratic outcomes. Voting mechanisms have broken down (vote via pop up ad) which has caused lack or representation and increased frustration particularly in rural areas. The anti-democratic party sees this as an opportunity to	leveraging platforms how they are intended (textbook content purchasing), inverse population targeting (middle country rather
	1	Purple Pawn	Corporations (information tribes) establish ownership over information - they are the controllers and governance of all information for purpose of market dominance. Throught this information dominance, major cultural divides emerge between information tribes, as well as between urban and rural populations. Those living closer to information hubs have access to virtual	information oligarchs, urban favoritism, information access divide (inverse),
	1	Black Pawn	Kai Foo Lee is a business tycoon with no permanent residence. Currently operating out of the Four Seasons Hong Kong (along with 44 well-armed security detail and 500 data scientists), his aim is to cleanse humanity and establish a new world order where the US is no longer a super power. Kai Foo Lee was driven to this extreme after loosing his wife and unborn twins to a misdiagnosis due to a faulty AI/ML algorithm within the US healthcare system. Since then Kai Foo Lee has cornered the market	passive manipulation, leveraging platforms how they are intended, personal vendetta, inverse population targeting (Iowa)
*	2	Red Pawn	Bobby Jo is a female first-class flight attendant from Atlanta and based in NYC with friends and connections globally. While in Athens posting on Instagram, a simple wifi spoof on her mobile device allows a N. Korea state sponsored actor (proxy to Russian private bio tech company w/ ties to Chinese cryptocurrency) to hack into her bio identification data. The N. Korean actors use her info to create a fast-mutating bio bomb for her to distribute as a bioweapon "Typhoid Mary". Now carrying a digital bio weapon, Bobby Jo infects others wherever she uses her bio ID, including TSA security personnel. Leveraging her security info, the N.Korean malactors pull the best infection vectors from airport system to propogate her virus to infect a targeted group, biofencing the infection to only US citizens within the FDA database. By targeting US citizens with a bioweapon, malactors are looking to eliminate US from the global leadership stage. In a world where everyone now has biochips implanted with biodata to help augment experiences (deeper movie experiences, etc.), bio-digital weapons can propogate quickly. After initial bio/geofenced dispersion, the second stange is PSYOPS - using the original Instagram account hack to deploy algorithms across social nets to (a) scrub mentions of biological /infection symptoms to decrease awareness of pandemic (b) create misinformation narratives about infected or uninfected demographics to drive blame, division and violence (e.g, 2030 census takers, dems or repubs, muslims, etc.). Given the misinformation campaign, virus spreads faster than truth across physical and digital encounters to infect a large portion of the US population, fanning hate as differently affected groups feed into multiple hate-based narratives ("well only dems are getting this"), the bio attack disables traditional medial forensics, and the wealthy elite are wiped out. Suriviors are people who opted out of chipping, or unable to be chipped (undocumentned immigrants survive) - creating an entirely new political, social, and economic landscape in the US.	leveraging platforms how they are intended (social connectivity), breaking the physical / digital divide (Real Mixed Reality), privaledge as vulnerability, new proxies of evil, microtargeting for systems access
	2	Orange Pawn	Joe Snuffy is a rural farmer in Taylor, Arizona. Since 2019, Mr. Snuffy has been disenfranchised, political matters that are important the rural communities dont make it to national platforms. This is futher exacerbated by removal of electoral college and a recent push to increase senate to represent more populous states, futher removing Mr. Snuffy and hiding confederates from their identity as Americans. In alignment with the growing succession movement in the SW USA, a vote in Arizonan rural communities resulted in overwhelming support for succession and union /alligience with Mexico. Mexico, backed by Russia / China after the completion of the Wall, sees this succession movement as an opportunity to break up the US via three joined adversaries. with a widening gap between local and national news, the Mexico/Russia/China conglomorate can target regions	new proxies of evil, siloed information as the new disinformation, exploiting a polarized environment, inverse population targeting (SW), individuals as pawns for global politics,
	2	Yellow Pawn	Carmine Santino is the 20 year old son of one of the prominant Families in Newark, NJ. The new, young, and idealistic District Attorney is running a campaign against the Santino family, wanting to reign in corruption - using AI to generate the entire video content in order to publicly push "Goober" (Uber for sustainable trash pickup) as a sensational idea generating lots of campaign money for public officers who support it. The DA doesn't yet grasp the connections that the mob controls and launhces a smear campaign on Carmine's father at a fundraising dinner by networking attendee's phones to collectively show a deepfake video of Mr. Santino talking about screwing over the sanitation workers. The DA wants to undercut the influence of the Santino family as part of the office's fight against corruption and mob control over economics. Through this smear deepfake, Carmine is "reflexively controlled" to take matters into his own hands in order to reestablish the Santino name before a second, much more impactful campaign is launched by the DA. He decides to hack all the original gadgets the state drew on to develop the AI fake and push the unaltered video to prove it was a fake and regain trust of the conglomerate. Unfortunately, data privacy laws has taken effect which has reduced anonymity of data. The legal environment has taken away civil liberties that makes government surveilance of individuals devices easier by tying internet enabled devices tied to biometric markers. The Supreme Court has reinterpreted privacy to individual not their devices or data. Carmine is caught in a loop of unprovable innocence, subject to the campaigns and word of the government via controlled data.	information oligarchs, organized crime inversion, data blackmail,

	Round	Team	Round Two - "Meaning" / "Insight"	Round Three - "Novelty"
	1	Red Pawn	system exploitation on two levels - data network (data systems, credentialing, logistica) and social network (emotional belief networks of employees, particularly those populations already feeling struggle) - creating synchornized doubt and vulenrability both soft and hard for a more pervasive attack.	emotional hacking in underlying systems / cultural exploitation
	1	Orange Pawn	anyone can be exploited. It's no longer those just with extreme/notable power or influence, but more and more those who simply have an audience (mid-fluencers)	individual psycho-targeting for military gain
	1	Yellow Pawn	priorities will always lie with cultural /social undercurrents - those things that are generations old and built into culture. Targeting vulnerabilities based on those cultural / social undercurrents will be exponentially more effective for reflexive control	psycho-targeting of country cultures to enable disorganization
*	1	Teal Pawn	information capitalism is the next iteration of disinformation dissemination / 'fake news'. Targeting moves from established decision makers to the	information oligarchs / information capitalism
	1	Purple Pawn	information access divide based on data capitalist practices. The same have/have not trope has shifted into an information access gap, exacerbating the	information oligarchs / information capitalism
	1	Black Pawn	control of pervasive non-critical data infrastructure (educational algorithms, textbooks, hiring practices) to behaviorally manipulate toward a single desired outcome. Those systems that are not top-secret are	information oligarchs / information capitalism
*	2	Red Pawn	blended biomimicry as a digital weapon. Taking cues from how nature works, both the dark side (pathogens, viruses, epidemics) and the light side (movement / communication networks, interconnected ecosystem webs) to create an attack that uses our natural human operation systems. Now intelligence can be sparked and let loose on a variety of levels for a variety of malintents. The creators may not even know what the desired end result may specifically look like.	biomimicry as an attack vector - leveraging design of natural systems (viruses, networks, natural organizational cues) across the biological, human, and digital worlds
	2	Orange Pawn	domestic conflicts become international vulnerability attack points. Splintering of domestic information dissemination is exploited by emerging conglomerates (either nations or corporations or both) to catalyze their own power goals.	domestic strife leads to international vulnerabilities, increased divisiveness creates political localism
	2	Yellow Pawn	government taking cues from criminal hacker activities to achieve overarching agenda items. "digital means to an end" mentality pervades across sectors grating a national Gothem City like environment where actions are taken by vigilantes also holding elected power.	Elected vigilantes

	2	Teal Pawn	Kaspar: Systems Admin / Developer for the major AR/VR corporation (off shoot of Huwaei), from Estonia. out-sourced worker; 30 years old; ran a fraudulent ICO scam in the past that screwed Estonia; lives alone with a pet rockAR - immersive environment that is personalized for individuals/communities; evolution of Netflix (infinite content available that is personalized to what you want); this becomes the battleground for the proxy war between India and China; AR gaming envionrment took off on Africa continent. given state of smart phone technology on the continent - makes this capable. compelling AR content is a mixture of gamified content and IRL competition. The content heavily relies on "the others" which motivates players to attack / gain an advantage over another group. The motivation for the game depends on motivating users against a perceived outsider threat that usually takes the form of unfamiliar strangers. Once the exploit is carried out, the opponent group becomes modifiable by attackers, and thus the motivations and emotions of users can be tailored against any group. India realizes this can advance their "hearts and minds" campaign against China and thus motivate local sentiment in their favor. US lost the trade war with China and are forced to allow Huwaei phones into the US. Resulting market share is that they are more popular than Andriod or Iphones. The US market is flooded with these devices. Indian state operatives (hackers, info war planners)A concerted effort to blackmail Kaspar in order to access and manipulate the core AR/VR alogirthm w/o the Huawei's knowledge. He was the developer behind a massive ICO scam that crippled the Estonian economy as they left the EU. Because flipped on his co-conspiritors interpol kept his identity secret and none of his immidiate network knows what he did. His immediate family is wrapped up in the Estonian nationalist movement. Extremely anti-EU and blames them for the economic collapse. His developer network is actively engaged in anti-EU activities. Sow civil unrest in the African continent to counter chinese successes. Specifically targeting African politicians and their families. Expose / frame African politicians as Chinese proxies. Creating dis-trust in the Chinese infrastructure that underpins their lives. Vulnerabilities: There is no way to determine the physical truth. Human vultrabilities in even the most secure technology. Indian hackers turn Kaspar by threatening to expose him for his role in the collapse of the Estonian economy. They push him to open up a door for them to inject their propoganda into the feeds for a two month period leading up to a big event. Broader Implications: Once the vulnerability is created it becomes a known exploit amongst hackers throughout the world. The vulnerable phones are in US and EU using the immersive content drive a massive amount of people into a known location. And given the love of the immersive event, they wont get off it even knowing that it is compromised.; New Threat Practices: Off-shoring development was a norm, creating broader networks of individuals with access to the technology. Less people around him to notice eratic behavior (because off-shore developer). Not enough oversight. ; Research Pipeline: Immersive content getting better, PokemonGo on steroids: social status and monitary insentives integrated intop the game. Smart phone and 5G improvement allows for Huawei phones to enable these experiences. Longer battery life enabling extended experience. Gates: Corporations tightly control access to and the development of feeds / algorithms, oversight by regulators; Transparency in the algorithms and operating systems of mobile devices makes it harder to hide malicious code / updates in plain sight; Data literacy increases through a function of generational change, increased skepticism of social media and extreme online content; Continue to prevent Chinese + foreign government consumer hardware from gaining traction in the West; Manhattan-style project bringing together industry + software experts to regain control of this broken arrow immersive content; Flags: The immersive content industry has legs and there are more than a handful of Pokemon-Go style successes – If Pokemon Go is Friendster, then there's some evolved version that has increased complexity and engagement ala Facebook; Increased opacity of the algorithms directing people's behavior IRL, and a decrease in corporate desire for transparancy; Decrease in domestic workforce, increase in off-shore developers with greater responsibility over core business logic and algorithms; Proxy battles between nation states increase in the information realm – India and China decide to fight it out with information not kinetics; Huawei winning access to the American market; Milestones (4 years): Discussion of transparency in aglorithms, funding for research of black box algorithm insight – NAS could fund researchers who work alongside social media company engineers to help public understand algorithms. GDPR-style audting of the algorithm's outputs is more important than its internal workings. Expectation that companies are protecting their secret sauce.; Government level support for teams to understand algorithms; decreased liability for more transparent algorithms; Investing in research that identifies effective tools and education for increasing digital literacy that can be handled to non-profits to be dissiminated ala international aid currently; Digital blue helmets: reserve engineers + scientists + sociologists willing to help foreign nations and other organizations mitigate damage caused by weaponized content and algorithms; Milestones (8 years): Former tech executives and engineers end up with public servant roles and have a vastly deeper understanding of how to regulate and legislate algorithms both domestic and foreign; Information warfare geneva convention established, able to identify China and India as violators.
	2	Purple Pawn	Kanye West - People of Color, Millenials, and former mainstream Trump supporters, leftwing voters, lives Primarily on left right coasts of the US, but also in Gulf Coast region for the first time.; Kanye narrowly loses 2028 election by .5% and declares election results subject to fraudRefuses to stop legally and socially contesting 2028 election results similar to Bush v Gore 2000. Organizes supporters to march on Washington DC in an organized protest that brings transportation, economic activity, and federal functions to a halt.Donald Trump who supports his friend Kanye, and Kim Kardashian.To cause a Constitutiuonal crisis. To lead a political fractionalization of the US along ideological-cultural lines. That a public backlash of these events will galvanize national unity and patriotism in the US. Vulnerabilities: Cultural, social, economic, political, and geographic fissures in the US.; Broader Implications: So the US can no longer act as a a global hegemon or leader for the West in international politics due to the fact that a fractured confederacy will not have the economic or military power to project as it currently does.; Info Delivery: Kanye West's campaign team uses personalized vignettes that conform to individual voter beliefs and preferences that are only delivered to an individuals' personal news and information feeds via advertising, social media, and print media. This prevents his coalition which is naturally internally fractured from fracturing, by never disclosing controversial policy stances or opinions from each other. Publicly, Kanye supporters only see valence issues, stances, or messages in public events where cross contatminations of information streams could occur - eg campaign rallies, protests. Additionally, public events not intended to cause chaos are carefully curated in who attends them in order to prevent friction between groups of supporters in public. Essentially, alternative facts have become alternative realities.; Barriers/Roadblocks: 1, Electoral college willl and should serve as a saftey net to prevent this issue, but it is undermined because multiple states across the country where the popular vote was within %0.1 have a number of faithless electors that do not conform to the popular vote in each state. Principally in Texas where Kanye wins the popular vote, but three electors vote for the Democrat incumbant. 2, The US Military/Law Enforcement/DHS serves as a barrier to the splintering of the US and the dissolution of the current constitution by enforcing martial law on behalf of the incumbant and to support adjudication of the election within the courts. 3, Hacktivists bring down contemporary media streams and interfere with personalized media content to present broader media picture to general public to dilute alternative information realities.; New Threat Practices: Personalized nano-targeting of audiences as blue and red as only version of reality, news, content (based on self political party identification). Whole room OLED screens in homes (the transition from living room to a media room) to create "virtual reality" and have the PResident talk with you, play games with you...brings new meaning to term "candidate can have a beer with". Reality is altered based on your political identity.; Gates: Institutions of government - military, supporters of traditional constitution and whole of U.S.; Media elite - all formats; Local Community - strong communities will diminish personalization effects; Big Tech; Flags: 2000 Bush v Gore - Palm Beach County, Hanging Chads; 2016 Election - Trump mainstreams the concept of Fake News and publicly begins undermining confidence in the impartiality and veracity of media coverage; 2016 Final Presidential Debate - Clinton asks Trump if he would abide by results of the election; Clinton loses, Democrats begin discussion undermining the legiticmacy and purpose of the Electoral College; Circa 2016 Kanye West aligns himself politically with Donald TrumpTrump appoints Kanye as ambassador to Russia; Dennis Rodman to North Korea; Voting goes to online only with fingerprint as identity proof; 2025 Trump formally endorses Kanye as Presidential candidate.; Milestones (4 years): Trump loses 2020 re-election bid and peacefully transitions government.; Convention between big tech and governemnt on ethics in media framing and delivery of ....;
	2	Black Pawn	Jackson Marsh, African American, Denver Police Chief of Denver Colorado USA ; China is facing a sustained Economic downturn, and decides to use AI and ML to disrupt the American voting process China micro targets US individuals inflaming passions and inciting support/organizing along "tribal lines" ANTIFA , BLM and local KKK affliated groups to start a misinfomation and disinformation campaign centered around voting thus giving rise to fringe party elements and those specilizing in identity politics The Chief is African American, also affected is his White Wife and his Bi Racial daughter that is attending college in NYC.China is seeking to create widespread chaos, distrust in an effort to suspend or delay the upcomming Presidential Elections - first time in US history. China wants to keep the incumbent administration in office. Vulnerabilities: Election Security, technical vulnerabilities of Social Media, Confidence in democratic insitutions ; Chief Marsh's daughter contacts him informing him that she has been notified via social media that large
**	3	Red Pawn	MAJ Diego Garcia, S2, intelligence Officer, Brigade Combat TeamM, Deployed to Madama, Niger, Africa (only city in NE Niger bordering Libya to the North and Chad to the East); China by proxy using radicalized groups out of Libya and Chad; China has large investment in Nigerios Oil and Hydro carbons. Niger is also deeply indebted to China as a result of loans for infrastructure projects. The Niger government is disintegrating under the weight of Chinese debt. The debt crisis has consequentially caused an Humanitarian crisis within Niger. As a result the international community, under the supervision of the U.N., has assembled Humanitarian Relief Operation to help Niger. These events have caused China to lose influence and substantial financial investment in Niger. MAJ Diego Garcia's brigade represents the U.S.'s support in this effort. The U.S. mission is to stave off humanitarian disaster and desolve Chinese influence in the nation. China's goal is to weaponize information in an effort to cause the U.N. task force's and more specifically the U.S.'s mission to fail.Coordinated digital and PSYOPs campaign to force MAJ Diego's brigade to withdraw from Madama without using controlled violence. Deep fake video's of U.S. Soldiers raping Nigerois woman and of U.S. security contractors summarily executing a remote Nigerios village (burning the village) on the outskirts of Madama which are proliferated through AI controlled chat bots on Chinese supplied 5G architecture. The most profound deep fake video depicts the beheading of a U.S. Soldier. This event both inspires local radical groups and creates dissent at home. The Chinese own and controll the information infrastructure which is leased to Niger. Huwai equipment are used in this infrastructure.Diego a mass of Madama citizens violently protest outside the brigade's base camp. A sniper from within Madama wounds a soldier during a presence patrol. Evidence of radicalized militant groups capable of enacting violence is appearing with intelligence reports from higher headquarters. China is creating virtual radical groups using virtual botnets that create solidarity with actual local radical groups inspiring action from them. The virtual radical groups are driven through AI driven botnets that uses digital exhaust, measures sentiment, and adjust its narrative without the intervention of humans. Deep fakes are timed to coordinate with supporting events such as farmers burning their fields after the normal harvesting process.Wife and children back home are scared. The children are crying and asking if the person in the video is their dad. U.S. public sentiment is becoming overwhelmingly opposed to the operation. China's goal is to weaponize information in an effort to cause the U.N. task force's and more specifically the U.S.'s mission to fail. Strategically China is looking to preserve their hydro carbon investment, long term secure rights to uranium deposits in the country (the world's largest). Prevent a restructuring of the Nation's debt (IMF bailout). Vulnerabilities: Secure encrypted information infrastructure (quantum) preventing a look at what is going on inside Niger. The Brigade's network for bandwidth purposes would have to connect to information infrastructure controlled by our adversary or competitor in the region. Authorities for capturing local social media data and higher presence on networks. Local's knowing we monitor their networks; however, due 5G technology they are able to create mobile ad hoc mesh networks that not trackable. ; Difference: Technological advances in 5G architecture, quantum encryption, the ability to automate high-quality, multi-view point,fake video, audio, and narrative; Broader Implications: It could cause de-stabilization in the U.S. Cost of deployment is greatly increase based on the technology (deploying the network), combat networks using organic 5G technologies that support not only troops but the local government and population. The use of AI technologies that cause ethical concerns and may compromise U.S. ideals. How do you properly credential US forces deployed to validate who you actually are, example distinguish between real and fake videos in the view of the local population?; Barriers/Roadblocks: Deploying and installing 5G architecture into a remote area like Madama is costly and cumbersome. They lack emotional and conscious (empathy) intelligence for establishing meaningful human relations with the local population. Cultural differences create obstacles geographically. Local and Niger government is resistant to Chinese influence. ; Business Models: Next generation entertainment models powered by 5G, customized by persoan preference models. Chinese cultural export and money influences local culture, improves local living conditions.; Gates: Develop mobile 5G information infrastucture (deployable). Portable controllable cyberspace.; Credential troops to distinguish between fake and real content (audio, video, and narrative).; Authorities to monitor flow over local information infrastructure; Develop the ability to detect 5G mobile ad hoc mesh networks; Signature management - the ability to monitor our own digital exhaust and media output. example Diego post a geo-tagged picture - or adversaries send fake beheading pictures to his family; Flags: Classic man-in-the-middle attack; Adversary controls the infrastructure - manipulate digital traffic between deployed force and home; Chinese space based systems - what they can see and analyze; The gap between the physical environment boundaries (geography) and boundaryless virtual environment; encrypted networks; Don't have control over local history; Milestones (4 years): Develop portable, cost effective, deployable 5G communications architecture; Organic human terrain teams (uniformed); Electronic warfare capabilities to detect ad hoc 5G networks; AI driven deep fake content detection; Virtualized units whose job is to produce local knowledge; secondarily create a conceirge like service to provide virtualized information to local populations based on local technologies; awareness and monitoring of local services; Milestones (8 years): Augmented reality for MILDEC purposes; deception to quell violent protest; fool satellites; Unbreakable encryption (quantum encryption?); Enhanced ability to validate networked communications over non-controlled (non-American) information infrastructure. ; Blockchaining, ledger technology for validation (non-repudiation).

	2	Teal Pawn	US lost the trade war with China and are forced to allow Huwaei phones into the US. Following trend, they are more popular than Andriod or iPhones and the US market is flooded with Huawaei devices. Alongside this change was the creation of a platform that evolved from Netflix called AR - an immersive environment for individuals / communities with infinate personalized content available which orignially launched in Africa given their investment in mobile technology over built infrastructure. Compelling AR content is a mixture of gamified content and IRL competition. The content heavily relies on "the others" which motivates players to attack / gain an advantage over another group. The driver for the game depends on motivating users against a perceived outsider threat that usually takes the form of unfamiliar strangers. Once the exploit is carried out, the opponent group becomes modifiable by attackers, and thus the motivations and emotions of users can be tailored against any group. India realizes this can advance their "hearts and minds" campaign against China and thus motivate local sentiment in their favor. In order to create a managed motivation, India targets Kaspar to access and manipulate the core AR/VR alogirthm w/o Huawei's knowledge. Kaspar is an outsourced systems admin / developer for the major AR/VR corporation (off shoot of Huwaei) who ran a fraudulent ICO scam in the past that screwed Estonia. Very few know of his ICO scam, which makes him a perfect target for India to blackmail into cooperation. Indian hackers turn Kaspar by threatening to expose him for his role in the collapse of the Estonian economy. They push him to open up a door for them to inject their propoganda into the AR feeds for a two month period leading up to a big event. Once the vulnerability is created it becomes a known exploit amongst hackers throughout the world. The vulnerable phones are in US and EU using the immersive content drive a massive amount of people into a known location. And given the love of the immersive event, they wont get off it even knowing that it is compromised. Ultimately, India is aiming to sow civil unrest in the African continent to counter chinese successes. Specifically targeting African politicians and their families. Expose / frame African politicians as Chinese proxies. Creating dis-trust in the Chinese infrastructure that underpins their lives through exploiting inability to determine physical truth.	microtargeting for systems access, programmable behavior, mob mentality, individuals as pawns for global politics, data oligarchs,
	2	Purple Pawn	Kanye narrowly loses the 2028 election by .5% and declares election results subject to fraud. He refuses to stop legally and socially contesting 2028 election results, and organizes supporters to march on Washington DC in an organized protest that brings transportation, economic activity, and federal functions to a halt. Feeling defeat, his aim is to cause a Constitutiuonal crisis – to lead a political fractionalization of the US along ideological-cultural lines believing that a public backlash of these events will galvanize national unity and patriotism in the US. Kanye West's campaign team uses personalized nano-targeted vignettes that conform to individual voter beliefs (blue or red) and preferences that are only delivered to an individuals' personal news and information feeds via advertising, social media, and print media. This targeting becomes the only version of reality, news, and immersive VR content - altering realities based on your political identity. This prevents his coalition which is naturally internally fractured from fracturing, by never disclosing controversial policy stances or opinions from each other. Publicly, Kanye supporters only see valence issues, stances, or messages in public events where cross contatminations of information streams could occur - eg campaign rallies, protests. Additionally, public events not intended to cause chaos are carefully curated in who attends them in order to prevent friction between groups of supporters in public. Given these divisions, the US can no longer act as a a global hegemon or leader for the West in international politics due to the fact that a fractured confederacy will not have the economic or military power to project as it currently does.	alternative facts become alternative realities, leveraging platforms how they are intended, digital life fracturing, exploiting diferences for political gain, mixed reality echo chambers
	2	Black Pawn	China is facing a sustained Economic downturn, and decides to use AI and ML to disrupt the American voting process China micro targets US individuals inflaming passions and inciting support/organizing along "tribal lines" ANTIFA , BLM and local KKK affliated groups to start a misinfomation and disinformation campaign centered around voting thus giving rise to fringe party elements and those specilizing in identity politics. China is seeking to create widespread chaos, distrust in an effort to suspend or delay the upcomming Presidential Elections - first time in US history. China wants to keep the incumbent administration in office. Chief Marsh (african american chief of police of Denver, CO) is torn between family and professional responsibilities. His bi-racial family is strained by ethnic tensions and tribalism - he personally looks forward to the federal election to bring	digital-kinetic blending, exploiting differences for political gain, data misdirection, alternative facts become alternative realities,
	3	Red Pawn	China is facing a sustained Economic downturn, and decides to use AI and ML to disrupt the American voting process China micro targets US individuals inflaming passions and inciting support/organizing along "tribal lines" ANTIFA , BLM and local KKK affliated groups to start a misinfomation and disinformation campaign centered around voting thus giving rise to fringe party elements and those specilizing in identity politics. China is seeking to create widespread chaos, distrust in an effort to suspend or delay the upcomming Presidential Elections - first time in US history. China wants to keep the incumbent administration in office. Chief Marsh (african american chief of police of Denver, CO) is torn between family and professional responsibilities. His bi-racial family is strained by ethnic tensions and tribalism - he personally looks forward to the federal election to bring leadership and stability, but the federal govt has announced the delay of the federal elections for a minimum of 12 months, a decision he is personally responsible to support and enforce. Chief Marsh comes out in public oppositon to the President's directive to delay elections and gains backing/support from the Colorado Governor (R) who announces that Colorado elections, including Federal ballot issues will be held using paper ballots. Following Colorado's lead states split in support or opposition to the (D) President's decision to suspend elections. Colorado Governor mobilizes the Colorado National Guard to ensure elections are held as scheduled. New York mobilizes their Guard to ensure elections are not held creating civil conflict over a large-scale misinformation attack.	alternative facts become alternative realities, programmable behavior, systems oligarchs (information oligarchs), new natural resources (information resources), information resource restriction (better word here), indirect military pressure,

**

	2	Teal Pawn	with increased availability and popularity of immersive technology systems, politicians take an increased interest in manipulating belief systems of large sections of citizens. Where propoganda in 1940s was overt and prideful, in 2010s was stream-of-conscious, in the 2020-30s it will become sub- or inter-consicous by leveraging immersive streaming platforms.	emotional hacking in underlying systems / cultural exploitation, propganda evolution
	2	Purple Pawn	the US slips into a semi-formalized split society along digital political echo-chamber lines. Without ability to cross digital dividing lines, US citizens only see a reality of curation - intended to speak to their identified digital personalities.	alternative facts become alternative realities, country lines evolving into digital political lines
	2	Black Pawn	exploiting the democratic platform to divide intent and interest in the process itself. Pitting the "social-media rumor mill" and those succeptible to it against political authority figures serves to widen gaps in the US democratic system - to the point where the original incindiary event is nearly forgotton. Malactors use our own domestic conflict to their favor.	alternative facts become alternative realities domestic strife leads to international vulnerabilities
**	3	Red Pawn	radicalized confirmation biases are elevated by exploiting the gap between pervasive deep fake technology and the ability to disprove their truthiness. Terrorist groups continue to leverage front-line tech platforms, and in this case deep fakes serve to create immediately enflamatory and radicalizing content. radicalization used as a distractor for political buisness practices and long-term nation power-grab planning	alternative facts become alternative realities, digially programmable physcial behavior

*	3	Orange Pawn	Joe Snuffy an E-7 in the US Army, Polish Military and other US Support personnel, Rotationally deployted to Fort Trump, with family at Fort Bliss.; Information Operations Units within the Russian Federation.VR training exploitation by Russian operatives that actively recruit, threaten, and solicit our Polish partners. Russians are able to do this via data harvesting from social media platforms One-on-one specialty targeting in the VR domain has
	3	Yellow Pawn	SGT Maria Sanchez, a Puerto Rican American, who was turned away from the border during Hurricane Maria in 2017, later enlisted in the Army, but still is bitter at the Trump administration for spurning Puerto Rican support requests. She is deployed to the California/Mexico border just south of the now underwater Imperial Beach area. During her work shifts, she controls a security checkpoint that receives dozens of live sensor feeds into a VR environment. Her rules of engagement allow her to fire upon any non-registered watercraft identified by the system entering into the contested waters. Deployed to CA/Mexico border but lives at Fort Hood, TX. A paid hacktivist that supports the movement for California to secede from USAFederal troops “accidentally “ fire on a mexican military border patrol boat due to a cyber attack on the US military person’s VR display and takes advantage of rules of engagement system difficencies. SGT Sanchez’s VR suite displays a watercraft that appears within the contested waters and registers it as a legal target for lethal engagement, because it has fully crossed the international border improperly. However, the system has been hacked to put a “okay to shoot” tag on a Mexican boat that is within its own territory.Her commander believes she acted correctly but there is a 15-6 investigation and in this process CID cyber analysis is finding conflicting and incunclusive evidences of cyber hacking on the SGT’s VR recording device. Files that should be stored are missing and while SGT Sanchez is fighting for her innocence inside UCMJ, some national media are putting her actions on trial in the court of public opinion. Want her to be the fall person. Want to push the rhetoric that California and US Federal system are incompatible, and sow public distrust. Vulnerabilities: Undermining trust in digital military network and battle space visualization tools for Military personnel. Undermining social trust in political leadership at local, state and federal levels. Undermining the international trust and agreements between Mexico, US and California. Racial and ethnic divides fuel mixed emotions for the fate of SGT Sanchez.; The Event: Coast lines shrink as climate change causes sea levels to rise. California is disgusted with Federal response to disasters on Caliornia coasts and groups begin movements to secede from teh nation. SGT Sanchez has all teh same physiological and psychological manifestations that occur whenever anyone is asked to make a decision to pull the trigger and end someone’s life. She also is feeling certain about her training on the VR sentry system, and has a hard time believing that such advanced tech could be wrong. She has feelings aboutte trust between her and her command as well as previous feelings of mistrust towards the federal gov’t when she wa a child, nd now she is being thrown under the bus of public opinion by the federal gov’t again.; Broader Implications: Broad implications of trusting digital tools in military decision making; dependence on civilian (or dual-use) telecoms architecture continues to reveal vulnerabilities of access to military systems; in the scenario, this inflames the resolve of pro-secessionist supporters for California to leave the nation. An external actor convinces her that they can help her examine the VR system to find the truth, but this is another layer to open vulnerabilities into military systems.; Research Pipeline: Inividualized and personal VR systems for each soldier that can be connected to the greater C2 or mission command networks; glide path for greater high speed broadband must continue and spectrum management must allow for wirelessly connected VR systems; VR transport (compression, etc) must develop so processing can be at the edge (at the individual soldier); Ecosystem Support: A hactivist would probably need insider access to either SGT Sanchez’s personal system (i.e. close personal access), to the connectivity backbone (i.e. thru wireless tech intercept), or through the public telecoms transport system; hactivist would also need massive support from pro-secessionist movement to ensure his actin were in line with their agenda; Gates: Rapid acquisition processes to field high-tech to soldiers and increase interoperability; Selection of companies who develop tech for military applications; Flags: States refusing to send troops to the borders in support of federal policies; President has to regain control over Right Coast Revolt; using federal troops is one tool - she has others; Insider actions / insider threat is still not perfectly mitigatable; Milestones (4 years): Trade tariffs, data privacy requirements, intellectual property requirements have begun bringing tech development back to the US —> leading to slightly increased control and trust over US-made tech; Anything to do to address climate change issues; Federal gov’t no longer subsidizes flood insurance for at-risk locations due to rising coastal waters; Milestones (8 years): AI-enabled scanning of networks for intrusions and hacks becomes more common; Federal acknowledgement that we did Puerto Rico wrong in the lack of support after Hurricane Maria; Education and emphasis on patriotism and national pride; Mechanisms (of whatever type...) to increase trust in democratic institutions.
*	3	Teal Pawn	Samantha, National Guard Soldier who is activated by the governor to quell unrest. She lives El Paso, Texas. Family situation? Her normal job is a social worker for the state ... this is "fringe-automatable" so worried about evolution of tech and the Chat Bot.US is more isolationist. We have lost our military advantage in the world. we are focused on keeping the peace at home now. nation states all have AI that puts us all in a stale-male for first action. Still dominate in nuclear capability but the battlefield with respect to information warfare / cyber we no longer have the advantage. Emotional therapy chatbots are military issue for all deployed personal to manage their mental health and be proactive about PTSD. Managing anxiety about
	3	Purple Pawn	National Guard active duty soldier - intelligence officer with access to electronic communications, Arizona native - Mexican American male 20 years old; Threat is Mexican Government; Emergency situation at Arizona-Nogales border declared by US President/Mexican President allegedly due to cartel murders; false flag of Mexican government conducting ethnic cleansings in border towns on both sides in Arizona and framing Cartel for it; incitive event is a shooting of Border Patrol agents at border check 20 miles from AZ-Mexico border.Martial law instituted in Mexico; US military brough in to enforce Mexican martial lawFamily is ranchers in the area on Mexican government want to seize territories back for Mexican posession. Vulnerabilities: US
	3	Black Pawn	Captain Avery Victoria, US Navy Virginia Class Fast Attack Submarine Commander - graduated 1st in her class from Annapolis, living in Yokosuka, Japan. Russia will create false tension in the region by spreading fake news and simultaneously manipulating US navy Senior arrays and on board maintenance systems. Increased Tension Between the USA/Russia and Japan. Capt. Victoria believes that she is defending the Japanese coast but she really sunk a Japanese naval vessel. US Govt Officials/ Japanese Govt Officials/her parentsRussia is seeking to decrease American presence in the Western Pacific. Russia is seeking to create tension between a newly independent Japan and the US Govt. The sinking of a Japanese vessel would

*	3	Orange Pawn		long term social/emotional manipulation, cognitive suggestive vulnerability, stereotype exploitation,
	3	Yellow Pawn	Joe Snuffy is an E-7 with the US Army being trained at Fort Trump with family at Fort Bliss. In 2029, the US and Poland militaries are using VR training modules to help prepare soldiers for deployment. Russian Information Operations Units are looking to create distance between the US and Poland, aiming to dissolve their alliance and reclaim the Baltic states. By targeting the VR system used for training across US and Polish forces, Russia can embed subliminal messaging into the personalized content delivered to each trainee. Blended into the default programming, Joe can't tell that he (and many others) are being targeted with specific messaging intended to sow discontent, depression, and distrust. The subliminal messaging able to be achieved via VR platforms is slowly transforming Joe's thinking about Poland, the Polish, and those he is training. The same is happening with Polish soldiers and how they think about the US. Interconnected VR systems linked with social media data enables increased ability for the immersive enviroment to do individual damage to Soldiers and to create individual worlds that degrade the commanality needed for training. As Polish and US forces mindsets begin to shift over time, Russia has created their own opportunity to reclaim Polish suppoert, and ultimately, territory and stature.	false triggers (using systems how they are intended via planting misinformation), leveraging unrest, martyr as decoy, system vulnerability targeting, microtargeting, cultural exploitation, us vs them triggers a political localism
*	3	Teal Pawn	In 2029 the US is increasingly isolationist. All nation-states now leverage an AI for decision making and first action, leading to the US having lost our military advantage and focusing on keeping trade agreements in place and maintaining peace domestically. While we still dominate with nuclear weapons, but are disadvantaged regarding cyber and information warfare. As red states like Texas flip to blue, civil anxiety is at an all time high. AI becomes seen as a solution for mental health issues both privately and publicly as the next evolution of telemedicine. Recommending chatbots instead of IRL talk therapy becomes easier	system vulnerability targeting, leveraging unrest, mental/emotional manipulation, manipulating behaviors for political gain, exploiting vulnerabilities in personalized platforms,
	3	Purple Pawn	An emergency situation erupts at the Arizona-Nogales border declared by US President/Mexican President allegedly due to a series of ethnic cleansing murders conducted by a local Cartel at towns on both sides of the Arizona-Nogales border. The incitive event is a shooting of Border Patrol agents at border check 20 miles from AZ-Mexico border. Matial Law is instituted in Mexico, US military brought in to enforce Mexican martial law. US media and intelligence is blind to what is really happening at the border. so Juan, an Arizona native and intelligence officer with access to electronic comms, is deployed to the border. All the	false triggers (using systems how they are intended via planting misinformation), leveraging unrest, cultural exploitation (US's desire to be protector), reflexive control,
	3	Black Pawn	Russia is seeking to decrease American presence in the Western Pacific. Russia is seeking to create tension between a newly independent Japan and the US Govt. The sinking of a Japanese vessel would compel the Japanese govt to ask the US military to decrease or abandon its military basing in that country. Additionally, Russia has been planting stories of atrocities committed by US military personnel throughout Japan.	reflexive control, leveraging platforms how they are intended, leveraging behaviors (military upbringing, cultural norms) how they are intended,

*	3	Orange Pawn	manipulation of belief systems through sub- or inter-conscious tailoring of messages delivered through pervasive immersive platforms. Directing behavior	emotional hacking in underlying systems / cultural exploitation
	3	Yellow Pawn	hightened military environments (increased defensiveness and nationalism) plus new technology systems leads to small, but impactful exploitation opportunities simply by manipulating one or two data points. A collection of small military "mistakes" rather than one large one leads to civil unrest and the reclamation of local governance power.	individual psycho-targeting for military gain, increased divisiveness creates political localism, digially programmable physcial behavior
*	3	Teal Pawn	leadership and decision myopia is spread through the manipulation of systems intended to be beneficial. Leveraging psychological manipulation (sub-conscious messaging and propoganda) to drive actions in line with one intended outcome.	emotional hacking in underlying systems / cultural exploitation
	3	Purple Pawn	governance systems using criminally-inspired tactics to create power-grabs. Psychological targeting of not just people, but countries dogmas in order to exploit common beliefs / practices / actions. US's stigma as having a "savior complex" is used against us to create	psycho-targeting of country cultures to enable disorganization, Elected vigilantes, digially programmable physcial behavior
	3	Black Pawn	simple data point manipulations lead to major miltary impact. Exploitation of the US training system and military organizational mantra assures human behavior even in uncontrollable (by malactor) circustances. Personal targeting not for blackmail purposes, but	individual psycho-targeting for military gain, digially programmable physcial behavior

	Round	Team	Round One - "Summary"
		Coon	Disinformation, Mal-formation, misinformation —> IDMs Tech advances (AI, smart cities, etc) can be used by adversaries to mechanize info to harm individuals and US AI/ML near complete automation - near real time adaption, mass scale, but personalized attacks Real-time + micro-targeting —> macro effects, at scale National, global, US security Incite violence & tribalism, anti-federalism —> question authority and relevance of US Distract populations, militaries, gov'ts —> focus on inflamed issues to gain advantage elsewhere Encourage individuals to move to violence Corporations —> increase profit, reach, competitive edge; cause harm to individuals and each other (corps.) Weaken union of US, education system, resilience of society
		Lin	Cyber-enabled warfare =/= cyber war Cyber war attacks tech & takes advantage of vulnerabilities in tech Cyber-enabled information warfare operations (IW) targets human mind (so does PSYOP & deception!) IW can use CW as means of content delivery Propaganda operations (false/true-false mix, to influence attitudes & emotions) Chaos producing ops (raise level of noise, inconsistent, distract) Hack & leak ops (hack is part of CW, but leak is also called Disinformation) Purposes (inform, distract, overwhelm attention, confusion, stimulate emotion) Human cognitive architecture (type 1 heuristics/intuitive/fast thinking, type 2 analytical/reflective/slow thinking) —> exploit difference is IW, esp by exploiting type 1 Cyber brings high connectivity, inexpensive production, democratized publishing, intermediaries no longer in place —> simplifies info warrior Filter bubbles (consume only info comfortable with) Lack of accountability, anonymity Attack methods (forged emails, videos, audio; highly selective targeting from leaked personal data; AI chat bots for radicalizing dialogue) Turn our strengths against us (U.S.) - i.e. first amendment allows for lots of people to shout in chaotic way —> differentiation between useful & inflammation
		Thomas	IO/CW/EW from Russian perspective Fake news, mimicry, deep fakes, spoofs Russia has gifted code writers & excellent mathematicians "Truth is a moving target" for Russia Success in manipulating mass media "Reflexive Control" - get someone to do for selves that actually they are doing for you (phishing is an example: they click on something they want but you get to deliver payload) Information packets prepared by special units inserted in battlefield (i.e. like good PSYOP units - look at moral situations of adversaries and try to exploit vulnerabilities) Information-technical & information-psychological elements Force state to make decisions favorable to Russia EW - potentially fake intercepts (i.e. reflexive control manipulation) Disorganization - deprive adversary from ability to accomplish combat tasks - key element in Russian doctrine that is absent in western doctrine Information weapons, struggle, strikes, confrontation —> words used in Russian IW Manipulate, destablize, destroy, provoke → these are all legitimate Russian military/IW objectives, not just techniques to a greater end EW - focus on NATO's weak space links, weak space force SODCIT - strategic operations for disruption of critical infrastructure targets EW brigades developing "disorganizing plan"; modeling adversary C2 to look for weak links "Soon" EW will decide fate of military operations (according to chief of Russian EW) Russia is comfortable with multiple versions of truth/how certain events unfolded History plays tricks on those who think it has ended - may be revisited "Information has become CoG for operations as much as power"; mass consciousness has been manipulated by information Deep fakes area of real concern; if video isn't liked, person can say "it was faked" —> liar's dividend EW spoofing to hide key facilities or mask movements of key people Escalation that gets out control; attack on critical infrastructure —> bother Russian planners the most
		DeCoursey	Consumer behavior Short-termism Media is fanning inflammation; we think "only people less smart than us are affected" Manipulation of masses Many others can use the tools of marketing, but aren't advertising campaigns Example of Egyptian internet trolls to create a media influence about Sudan massacres Line between advertising and propaganda is very thin; individualized targeting pushes us over the line Marketing firms and methods are complicit in many negatively viewed activities (war, free porn, objectification of women, racial/gender stereotypes, tobacco addiction, etc) Targeting the individual; "solitary confinement of information" "What if all advertising must have witnesses?" Fear of trajectory of mass marketing —> not just data privacy, but personalized targeting Is the tension worth the value we are creating?
		Reed	Narrative around data, esp. in elections "Data exhaust" or "social exhaust" that comes from our devices; we are being targeted by everyone (corps, NGOs, non-profits) Targeting is everyday, all the time b/c of our data As we give out more data, does AI weaponize it sooner Are we collaborative with our data? People are not aware we are pushing out all the data (exhaust) but even if we are aware they don't care
		Wieser	Access content increasingly - mostly social media, but also digital platforms (apps, etc) TV/radio will continue (esp. for older populations) but will diminish importance Word of mouth (no money applied) but probably most important distribution of info (amplified delivery from other means) Immersive digital experiences (AR/VR) plus avail. Of faster broadband increase Challenges to info distribution: "news desert" (journalism hollowed out as print publishers failed to adapt business models, but national journalism is very high quality —> topics of national importance never better, but local importance topics never worse) Lack of depth in local/regional information b/c no funding Disinformation will get worse, fake news Distrust of news & information more generally Leaders vilify reporting they don't like; misuse of terms; mistrust of whole ecosystem —> during real national crises, people won't know who to trust Deep fakes will continue Solutions: social media platforms self-imposed "know your customer" rules; consumers demanding knowledge of what is placed on their platforms; legal changes causing social media to "have to care" Solution: Social media literacy could increase - know how news is produced, quality of production, how to independently check facts (gov't or otherwise take action to increase media literacy)
		Allenby	Trends in IW: think broad in scenarios we consider (think difficult & ridiculous) —> b/c of speed of tech evolution Black Mirror showed social credit score, 2 years later China implemented it Immediate immune response of west to i.e. Russian disinformation camp has begun —> needs to continue, but NOT sufficient What do we do when Russia combines Cambridge Analytica plus CGI/deep fakes for 2020 election Also think longer term thinking @ changes in IE: issues of free speech have become "privatized" —> Twitter, Facebook, YouTube have as much to say about free speech as do our courts We are not Prepared for attacks against democratic institutions; what fundamental weaknesses are exposed by variety, speed of information? Favors soft authoritarianism
		Greer	Managing data in fully connected state AI is very different than any other tech on the battlefield —> data vs data; AI/algorithms vs AI/algorithms —> all fully connected [I can see an entire short story written about the "algorithm wars" waged by machine vs machine and not a single human aware it was going on, let alone harmed] Gap in data literacy —> find ways to make warfighter literate at every level International competitiveness and cooperation: non-tech issues (i.e gap in education must be closed; focus on inequality of income gap to meet challenge of AI -enabled warfare; also focus on data literacy) Focus on innovation: convergence on biomimicry, cognitive enhancement, neuromorphic capabilities (i.e. learn in new ways) [are these new attack vectors for IW?] Augmented, virtual, physical worlds merge —> global communication platform Responsible & ethical use of AI as humans become stronger, faster, enhanced —> focus on "should we" more than "can we" anymore No existing playbook @ privacy, CW, social media data, ethical conundrums from AI

	Round	Team	Round Two - "Meaning" / "Insight"	Round Three - "Novelty"	
		Coon	Manipulation of the masses through automated, individual targeting on a mass scale; Distraction from real issues leads to weakening of US critical values	Distracting the parts distracts the whole	"IDMs" are short-hand for the social/cultural manipulation method that is largely within the private sector; uses visible data and data exhaust for business, advertising, emotional manipuation, but is a GAP for military operations
		Lin	Vulnerabilities in the human mind become the mechanism to stir the pot; Data is porous at the borders, yet jurisdictions are constrained; Cyber-supported IW is used to get sensitive & private information out of the shadows to sow chaos; People's realities will be shaped and informed by automated bots and processes	Cyber-supported IW	Information maneuver is more than IDMs; EW manipulation of the signal and cyber manipulation of both data and conduit are all valid legs of the IW stool
		Thomas	Russia is very comfortable with multiple versions of truth at the same time - yet the US is not; Creating chaos is an end to itself, but the best IW leads to control (reflexive control); There are both technical (EW, cyber-enabled) and psychological channels to IW effects and both can be manipulated; Russia is willing to play the long game and is willing to remember history that has long passed under the bridge for the US	Truth as a moving target; Chaos is an ends to itself	Aims of IW for adversaries may not be an ordered world, because that keeps the US in control
		DeCoursey	Marketing and media has been weaponized - marketing has been complicent in creating many forms of shameful history; People ARE the products; Targeting subconscious anxieties and emotions (shame, judgement, vanity, etc.) is highly manipulative and abusive, especially if you are the only one who can see your version of reality - All advertising must have winesses; Digital addiction will continue to be monetized and pursued;	People are the products	How does the Army tap into this aspect of the IDM?
		Reed	Weaponization of our digital exhaust is just as prevelant as weaponizing our purposeful digital activities; Collection and exploitation of latent data is going to continue to rise	Weaponization of digital exhaust	The "visible" data is the easier set to wall off and manage, yet the "invisible" data is just as pernicious, and may even show more of a person's vulnerabilities to psychological manipulation
		Wieser	Decline of traditional journalism, yet word-of-mouth amplified by digital delivery will continue to rise; 5G and faster connections will increase the volume but not necessarily the quality of information; Idea of a "news desert" that highlight topics of hot conversation nationally but reduction of local & relevant news; Visual information will be more resonant (video, VR/AR); Are media content providers going to become gatekeepers of truth?; Need more data literacy training & ways to independently check facts	Platforms as gatekeepers	Ties with data oligarchs; whoever controls the data repositories OR whoever controls the algorithms that mine them and make sense of the data will be the ones who control the IDM; What are the platform responsibilities towards free speech, detection & censorship of fake news?
		Allenby	Issues of free speech have become privatized; Social media platforms become gatekeepers; Soft authoritarianism is needed to "control" rampant untruths	Platforms as gatekeepers	same as above
		Greer	Fully connected world; Algorithm vs. algorithm warfare; Decline of US military superiority; Gaps in education, income inequality, data literacy contribute to decline of US superiority; AR/VR more than games - will be used in warfare; Responsible and ethical uses of AI not finalized; No existing playbook means new institutions required	Decline of US superiority	"Phoenix" syndrome - decline of civilizations often lead to a new creature that is strong and vibrant

		Cole	Not possible to create perfect rendering of future, but striving to avoid certain things matters as well Fragmentation of personal realities → increasingly impersonalized electronic relationship with consciousness (collective & individual) Ability to shape and wield different realities to gain tactical advantage Make a tank look like a garbage truck, using tech, VR/AR How does this get done? Engineered social constructs for control and stability (China) One belt, one road Conduits that individuals have access to because of AR/VR → think of the personalized interpretation of the Beijing Olympics you could see when the gov't airbrushes out smog and controls the social media feeds of athletes complaining of hacking coughs Privatization of private security (more than physical forces) → matrix of public/private forces Data becomes the "marching force" rather than helicopters Rent proxies for short periods of time to create effects → what are the boundaries and rules? Is western world comfortable knowing and breaking the rules Need for small teams to locate individuals (i.e. in dense urban environ) using commercial data rather than traditional intelligence → useful for targeting New standards and norms that may be broken from time to time How do we trust what we see and know; how do we trust forces deployed; how do troops trust machines alongside them? Trust cycle is slower than rate of change Thinking about unanswered questions → what is info domain equivalent to banned weapons (i.e. campaign to ban robots on kinetic side) and legal/ethical questions and conversations around information

		Cole	Fragmenting personal realities; Impersonal relationships with each other; Reality shaped by the tech we surround ourselves with; Countries will selectively create and display the truths that fit their worldview; Data will be the weaponry of the future and it will come from latent as well as purposeful activities; Privatization of national security; Speed of conflict will be so rapid we may miss it	Privatization of information security	Who are the data oligarchs and how does the Army use the data for their purposes? Processes, legalities; Data abroad vs. data on US citizens and activities that are threats within US borders

	Round	Team	Round One - "Summary"	One - "Summary	initial themes
	1	Red Pawn	young mother, 1st nations community, rural community, Pad, artist - Bailey - born 2009; Paducah, KY - 3rd most prominent micropolitan// shipping transport - Walmart; Chinese multinational wants to interdite; Chinese multinational creatres social media narratives - recycled memes, old stories about shabby product, underpayment of workers - first native american, then other subgroups, including the head of logistics, use AI autogenerated communities of fake workers complaining. emails and messages are interdited with a phishing attack disguised as a link to the AI genreated Audio/video deep fake "exposee" videos - to secure logisitcs/operations credentials - also bots targets workers	A young mother ir	system vulnerability targeting, microtargeting, primary targets / secondary markets, private lives / professional impact (private professional blend),
	1	Orange Pa	Joe Snuffy - social media influencer at a univeristy; Low econmic community in the suburbs of st. louis; Deep Faked podcasts using his voice, similar enough to his topics the make it impossible to deny; People are questioning his new views, peers disassoiate, univiersity questions motives. Starts panicing; close family, significant others; they want to use the legitamacy of the podcast to disseminate their message; Vulnerabilities: truth verification	Joe Snuffy, a soci	mid-fluencers (medium-fame influencers) as platforms, exploiting normalcy, make it and break it
	1	Yellow Pa	Akito Naruhito, decendent of emperor Naruhito of Japan; Climate change is influencing Japanese strategic decisions to consider new territory to enable national/cultural surivival; Akito is a target of Chinese IW trying to divide her (as an influential political and military symbol) away from achieving Japan's "first boots on land" strategy in China; Akito is the daughter of the throne reestablishing the Empire and dominance of Japanese culture through the pacific. She's responsible for establishing the resurgent warrior culture in Japanese culture; Akito's daughter is 7, and has grown up in a	Akito is the daugh	microtargeting, private lives / professional impact, cultural exploitation, emotional hacking
*	1	Teal Pawn	Middle School Civics teacher; Mrs. Foley; older gal that remembers how democracy used to work in the early 2000s; Iowa; Refugee camp as there is only 1 farmer left in the area; Mrs Foley gets targeted to purchase textbooks that are re-writing history as anti-democratic party is changing society; influenced to burn old textbooks that might "correctly" describe history; in the future everyone's textbooks are personalized and open to the highest bidder for content - so, in real time - changing content exists ... all of which makes it hard for her to consistently teach; additionally, grading is out of her control as AI grades assignments; also, deep fake videos to change history (like George Washington says) real-time as people bid: the anti-democratic party is starting to take power	Mrs. Foley is a mi Influenced throug	leveraging platforms how they are intended (textbook content purchasing), inverse population targeting (middle country rather than coasts), reality manipulation, inductive learning bias, passive manipulation
	1	Purple Pa	Corporations + Information tribes/ Haves Have nots due to infrastructure access; Urban/suburban/virtual = first world of US; rural, poor access; reservation = third world of US; Huge divide between tribes and urban vs. rural; Experience life as a non-citizen, cannot participate in society (politically, economically, socially, knowledge) fully ; Want to achieve information dominance - they are the controllers and governance of all information for purpose of market dominance. Corporate nation side; corporatism; Vulnerabilities: threatens exsitence of current liberal democracy; Haves: apps, social media, messaging, virtual worlds that incorporate social; mind melding	Corporations (info	information oligarchs, urban favoritism, information access divide (inverse), sell self for access, information socialism, tech as divisive decisioning
	1	Black Paw	Kai Foo Lee CEO and evil mastermind ; No country of residence - lives everywhere and lives nowhere (currently residing in Four Seasons Suite in Hong Kong) along with his 44 well armed security detail and 500 data scientists.; Cornered the majority of AI/ML technology; controls education systems and hiring practices of all technology companies worldwide through his algorthmtic approach to everythingKai Foo Lee's love of life was misdiagnosed due to a fault AI/ML algorthrym in the US Healthcare system and lost her life as well as her unborn twin boys.Several unknown mistresses and his daughter who is the heir apparent for his global empire. Her birth mother is a Uyghur and lives off the grid converting feces into electricity further perpetrating the	Kai Foo Lee is a t	passive manipulation, leveraging platforms how they are intended, personal vendetta, inverse population targeting (Iowa), exploiting normalcy, tech as divisive decisioning
*	2	Red Pawn	Bobby Jo, female flight attendant, visiting Athens Greece, 28 yr old, from Atlanta, based in NYC, the b	Bobby Jo is a fem In a world where	leveraging platforms how they are intended (social connectivity), breaking the physical / digital divide (Real Mixed Reality), privaledge as vulnerability, new proxies of evil, microtargeting for systems access
	2	Orange Pa	Joe Snuffy, Rural farmer, Citizens of rurual communities from Taylor, Arizona; Offers from state actors in Mexico creating allies with Southwestern Farmers to potentially secedeMexico with Chinese/Russian help. The United States has been successfully countering Russian and Chinese information operations with AI and better cyber tools. However, since the completion of the wall, Mexico now sees the US as an adversary and the Russians/Chinese see an opening with Mexico as a proxy to get tanglible results from an IO. The growing secession movement in the US Southwest is	Joe Snuffy is a ru Offers from state	new proxies of evil, siloed information as the new disinformation, exploiting a polarized environment, inverse population targeting (SW), individuals as pawns for global politics,
	2	Yellow Pa	Carmine Santino, son of one of the 5 families; age 20, supervises logistics systems at the docks in Ne	Carmine Santino Through this sme	information oligarchs, organized crime inversion, data blackmail,
	2	Teal Pawn	Kaspar: Systems Admin / Developer for the major AR/VR corporation (off shoot of Huwaei), from Esto	US lost the trade Indian hackers tur	microtargeting for systems access, programmable behavior, mob mentality, individuals as pawns for global politics, data oligarchs,
	2	Purple Pa	Kanye West - People of Color, Millenials, and former mainstream Trump supporters, leftwing voters, liv	Kanye narrowly lo Kanye West's can	alternative facts become alternative realities, leveraging platforms how they are intended, digital life fracturing, exploiting diferences for political gain, mixed reality echo chambers
	2	Black Paw	Jackson Marsh, African American, Denver Police Chief of Denver Colorado USA ; China is facing a su	China is facing a	digital-kinetic blending, exploiting differences for political gain, data misdirection, alternative facts become alternative realities,
**	3	Red Pawn	MAJ Diego Garcia, S2, intelligence Officer, Brigade Combat TeamM, Deployed to Madama, Niger, Afri	Niger is deeply in The Chinese own This radicalizatior	alternative facts become alternative realities, programmable behavior, systems oligarchs (information oligarchs), new natural resources (information resources), information resource restriction (better word here), indirect military pressure,
*	3	Orange Pa	Joe Snuffy an E-7 in the US Army, Polish Military and other US Support personnel, Rotationally deploy	Joe Snuffy is an E	long term social/emotional manipulation, cognitive suggestive vulnerability, stereotype exploitation,
	3	Yellow Pa	SGT Maria Sanchez, a Puerto Rican American, who was turned away from the border during Hurrican	SGT Maria Sanch SGT Sanchez's p As climate chang	false triggers (using systems how they are intended via planting misinformation), leveraging unrest, martyr as decoy, system vulnerability targeting, microtargeting, cultural exploitation, us vs them triggers a political localism
*	3	Teal Pawn	Samantha, National Guard Soldier who is activated by the governor to quell unrest. She lives El Paso	In 2029 the US is Samantha is a Na Behind this shift ir	system vulnerability targeting, leveraging unrest, mental/emotional manipulation, manipulating behaviors for political gain, exploiting vulnerabilities in personalized platforms, programmable behavior,

Round Two - "Meaning" / "Insight"	BDJ Notes	How to Relate to Broader IW	Round Three - "Novelty"		
system exploitation on two levels - data network (data systems, credentialing, logistica) and social network (emotional belief networks of employees, particularly those populations already feeling struggle) - creating synchornized doubt and vulenrability both soft and hard for a more pervasive attack.	THREATS: Data attacks / Social attacks stoking EXISTING doubt/fear/belief (CONDITION)	Data / IDM	emotional hacking in underlying systems / cultural exploitation	ali: add "labels" to each threat futur	
anyone can be exploited. It's no longer those just with extreme/notable power or influence, but more and more those who simply have an audience (mid-fluencers)	WHO: mid level influencers (anyone can use)	IDM (anyone can use)	individual psycho-targeting for military gain		
priorities will always lie with cultural /social undercurrents - those things that are generations old and built into culture. Targeting vulnerabilities based on those cultural / social undercurrents will be exponentially more effective for reflexive control	THREATS: targeting broader culture	IDM (culture hacking)	psycho-targeting of country cultures to enable disorganization		
information capitalism is the next iteration of disinformation dissemination / 'fake news'. Targeting moves from established decision makers to the emerging decision class - hyjacking their thoughts before they are formed.	Information Capitalism / THREAT: passive (long term) manipulation at scale but personalized	Long term IDM / Digital hack	information oligarchs / information capitalism		
information access divide based on data capitalist practices. The same have/have not trope has shifted into an information access gap, exacerbating the instability shared information for governance decision making.	Information oligarchs / CONDITION: urban/rural	IDM	information oligarchs / information capitalism		
control of pervasive non-critical data infrastructure (educational algorithms, textbooks, hiring practices) to behaviorally manipulate toward a single desired outcome. Those systems that are not top-secret are now the most vulnerable and most valuable.	THREAT: manipulate "gray zone"	IDM / Data	information oligarchs / information capitalism		
blended biomimicry as a digital weapon. Taking cues from how nature works, both the dark side (pathogens, viruses, epidemics) and the light side (movement / communication networks, interconnected ecosystem webs) to create an attack that uses our natural human operation systems. Now intelligence can be sparked and let loose on a variety of levels for a variety of malintents. The creators may not even know what the desired end result may specifically look like.	CONDITION: Crumbling of Digital and physical barrier	Digital and biological blended attack	biomimicry as an attack vector - leveraging design of natural systems (viruses, networks, natural organizational cues) across the biological, human, and digital worlds		
domestic conflicts become international vulnerability attack points. Splintering of domestic information dissemination is exploited by emerging conglomerates (either nations or corporations or both) to catalyze their own power goals.	CONDITION: urban ruals / THREAT: use of domestic conditions to grain advantage by foreign actors	IDM	domestic strife leads to international vulnerabilities, increased divisiveness creates political localism		
government taking cues from criminal hacker activities to achieve overarching agenda items. "digital means to an end" mentality pervades across sectors grating a national Gothem City like environment where actions are taken by vigilantes also holding elected power.	use by government against criminals	IDM (who: digital vigulanties)	Elected vigilantes		
with increased availability and popularity of immersive technology systems, politicians take an increased interest in manipulating belief systems of large sections of citizens. Where propoganda in 1940s was overt and prideful, in 2010s was stream-of-conscious, in the 2020-30s it will become sub- or inter-consicous by leveraging immersive streaming platforms	CONDITION: Rise of immersive tech capabilities and use	IDM / Data - Data / IDM - CONDITION: AR	emotional hacking in underlying systems / cultural exploitation, propaganda evolution		
the US slips into a semi-formalized split society along digital political echo-chamber lines. Without ability to cross digital dividing lines, US citizens only see a reality of curation - intended to speak to their identified digital personalities.	alternative facts become alternative realities, leveraging platforms how they are intended, digital life fracturing, exploiting diferences for political gain,	IDM	alternative facts become alternative realities, country lines evolving into digital political lines		
exploiting the democratic platform to divide intent and interest in the process itself. Pitting the "social-media rumor mill" and those succeptible to it against political authority figures serves to widen gaps in the US democratic system - to the point where the original incindiary event is nearly forgotton. Malactors use our own domestic conflict to their favor.	CONDITION: exisiting problems enflamed / FA uses to destabilize	IDM / Data	alternative facts become alternative realities domestic strife leads to international vulnerabilities		
radicalized confirmation biases are elevated by exploiting the gap between pervasive deep fake technology and the ability to disprove their truthiness. Terrorist groups continue to leverage front-line tech platforms, and in this case deep fakes serve to create immediately inflamatory and radicalizing content. radicalization used as a distractor for political buisness practices and long-term nation power grab planning	Articulated IW scenario	IDM / Data / Physical / Signal? / Psy - ops	alternative facts become alternative realities, digially programmable physcial behavior		
manipulation of belief systems through sub- or inter-conscious tailoring of messages delivered through pervasive immersive platforms. Directing behavior through subtle subconscous	THREAT: long term social / emotional manipulation / CONDITION: Rise of AR/VR	IDM - CONDITION: AR/VR/MR	emotional hacking in underlying systems / cultural exploitation		
hightened military environments (increased defensiveness and nationalism) plus new technology systems leads to small, but impactful exploitation opportunities simply by manipulating one or two data points. A collection of small military "mistakes" rather than one large one leads to civil unrest and the reclamation of local governance power.	CONDITION: AR/VR/ML / used by state actor	Data / IDM - CONDITION: AR/VR/MR	individual psycho-targeting for military gain, increased divisiveness creates political localism, digially programmable physcial behavior		
leadership and decision myopia is spread through the manipulation of systems intended to be beneficial. Leveraging psychological manipulation (sub-conscious messaging and propoganda) to drive actions in line with one intended outcome.	CONDITION: AR/VR/ML / used by state actor	Data / IDM - CONDITION: AR/VR/MR	emotional hacking in underlying systems / cultural exploitation		

	3	Purple Pa	National Guard active duty soldier - intelligence officer with access to electronic communications, Arizona native - Mexican American male 20 years old; Threat is Mexican Government; Emergency situation at Arizona-Nogales border declared by US President/Mexican President allegedly due to cartel murders; false flag of Mexican government conducting ethnic cleansings in border towns on both sides in Arizona and framing Cartel for it; incitive event is a shooting of Border Patrol agents at border check 20 miles from AZ-Mexico border.Martial law instituted in Mexico; US military brough in	An emergency sit Turns out the Me	false triggers (using systems how they are intended via planting misinformation), leveraging unrest, cultural exploitation (US's desire to be protector), reflexive control,
	3	Black Paw	Captain Avery Victoria, US Navy Virginia Class Fast Attack Submarine Commander - graduated 1st in her class from Annapolis, living in Yokosuka, Japan. Russia will create false tension in the region by spreading fake news and simultaneously manipulating US navy Senior arrays and on board maintenance systems. Increased Tension Between the USA/Russia and Japan. Capt. Victoria believes that she is defending the Japanese coast but she really sunk a Japanese naval vessel. US Govt Officials/ Japanese Govt Officials/her parentsRussia is seeking to decrease American presence in the Western Pacific. Russia is seeking to create tension between a newly independent Japan and the US Govt. The sinking of a Japanese vessel would compel the Japanese govt to ask the US	Russia is seeking Captain Avery Vic Captain Victoria b	reflexive control, leveraging platforms how they are intended, leveraging behaviors (military upbringing, cultural norms) how they are intended, blended attack (general + specific, social + technical), private lives / political + professional impact,

governance systems using criminally-inspired tactics to create power-grabs. Psychological targeting of not just people, but countries dogmas in order to exploit common beliefs / practices / actions. US's stigma as having a "savior complex" is used against us to create an opportunity for military gain.	CONDITION: Leverging unrest / false triggers to gain military/state opportunity	IDM	psycho-targeting of country cultures to enable disorganization, Elected vigilantes, digially programmable physcial behavior		
simple data point manipulations lead to major miltary impact. Exploitation of the US training system and military organizational mantra assures human behavior even in uncontrollable (by malactor) circustances. Personal targeting not for blackmail purposes, but instead for psychological understanding and behavior manipulation.	THREAT: micro targeting soldier / CONDITION: AR/VR	Data / IDM - CONDITION: AR/VR/MR	individual psycho-targeting for military gain, digially programmable physcial behavior		

Label (goal of 7 +/- 2 labels)	Description/Definition	Indicators or Flags	Examples
alternative facts become alternative realities	immersive content becomes the only content, yielding ever more real worlds that are based on virtual curation of biases	free speech is privatized (intellectual solitary confinement), continued split of communication channels (on party lines), reliance on immersive technology as communication dissemination platforms	extreme information divide particularly to take down democratic process (purple pawn 2, black pawn 2) and to seed discontent to open up business lanes (red pawn 3)
domestic strife leads to international vulnerabilities	an increased splintering of US information sources creates active vulnerabilities for international power grabs	free speech is privatized (intellectual solitary confinement), continued split of communication channels (on party lines), formation of new international conglomerates (mexico / china / russia)	china stalling election through misinformation (black pawn, 2) and emboldened secession movement (orange pawn, 2)
emotional hacking in underlying systems / cultural exploitation	targeting cultural undercurrents as vulnerabilities to be exploited particularly through subconscious messaging - leading toward one mal-intended outcome (either by minority or external force).	exploitation of neutral gaming systems for messaging (emotional connectivity through gaming platforms), investing in media literacy	sub- or inter-conscious propaganda (orange pawn 3 and teal pawn 2 and teal pawn 3, red pawn 1)
individual psycho-targeting for military gain	psychologically profiling individual targets to manipulate their actions through understanding cultural upbringings and belief systems, particularly when acting within a military construct	increased targeted advertising, political recommendations via google ads, investing in media and data literacy	sinking a japanese ship she thought was russian (black pawn 3), sinking a friendly ship she thought was hostile (yellow pawn 3), non-military podcast propaganda (orange pawn 1)
psycho-targeting of country cultures to enable disorganization	psycho-analyzing a country can lead to exploitative opportunities based on the prevailing dogma within that cultural system	investing in media literacy, misinformation campaigns around countries rather than individuals	US savior complex (purple pawn 3), japanese familial honor (yellow pawn 1)
information oligarchs / information capitalism	owned information creates an information access divide, particularly surrounding the urban / rural split	investing in data literacy at every level, extreme or hightened urbanization, creation of an explicit data market	information capitalism - text book content manipulation (teal pawn 1) info oligarchs and urbanized access priority (purple pawn 1), control of non-critical infrastructure toward large scale behavior manipulation (black pawn 1)
Elected vigilantes	taking cues from hacktivist campaigns, government enters a new era of social and political manipulation	degredation of political action oversight ("the law doesn't apply to me" mentality)	govs taking cues from criminal actors (yellow pawn 2), and govs acting like criminal actors (purple pawn 3)
increased divisiveness creates political localism	with increasing debate and difference, states and local governances believe they are better served as small groups rather than by a national disinformation machine	local laws gain more support than national or constitutional laws, state constitutions override federal decisions, campaigns like "cascadia", "jefferson state", or toward a seceeding california pop up all over the nation in increasing numbers	military mistakes leads to national government distrust (yellow pawn, 3), information siloing leads to succession talks (orange pawn, 2)
bio / digital divide (biomimicry as an attack vector)			red pawn 2
		portable genetic engineering tools (CRISPR)	
		Global IOT prototcols	
		biometric identification implanted	

Next Steps
can this lever be used both ways? if the concept is a threat to the US, can the US also use it against others?
call out in report successes/challenges in previous attempts at doing this in US military
experts to help us understand what cultures a country has; or whether there are slices of cultures
See Nathan Shedroff, re: finding that 6-7 companies world wide own the algorithms that create chatbots and voice bots
do we need to discuss the right/wrong vs legal/illegal uses of techniques?

								For Monday 10/21					
Report Overview								IW definition					
	Exec Summary, etc							Start to do some writing. use as few words as possible. "this is what the data says"					
	Introduction							think about red pawn 3 - blended					
SME overviews								get some flags / gates down					
	summaries per person							get first draft down and pass back to BDJ / Jason					
IW Introduction								**After Monday 10/21**					
	definition of IW												
	"framework" of IW - we only really hit on IDM, what other areas exist (for further investigation)?						we have investigated the future of it. a lot have fallen under social/cultural						
	definition of IDM / area that we focused on for this report (what fits in / what doesn't)												
	main take-aways for IDM found through the Threatcasting Worksession												
Selected scenarios													
	3-5 ish												
Threat areas													
	Overview												
	brief definitions												
	the threats broken down		tying to Information Maneuver (its the application of IW to the fighting force - aka how would a commander use IW in battle offensive, defensive, etc. - making it more operationa										
	"novelties" as threat vectors / subbullets / examples of larger threats (one paragraph per novelty)												
	examples (call out which threat futures you think best describe the definitions)												
Threat actors													
	tbd whether we need a separate section...												
OPSEC Analysis	Of results as a thought experiment												
Next Steps													
	Flags												
		Social / culture	(if people are attacking those who feel underserved, how do we figure out who feels underserved? challenge for academia?)										
		Tech	(AR, VR, MR)										
		Economic											
		Environmental											
		Political											
	Gates												
		Military	look at all of these tech platforms to articulate intended and unintended uses (herb's definition explained). look at stated use and potential threat use										
			we need to change the definition of the character of warfare - pull language from google doc initial findings IW										
		Gov											
		Academia	look at all of these tech platforms to articulate intended and unintended uses (herb's definition explained)										
		Private Sector											
		Non-profits											
		citizens											
Summary / Conclusion	Lab's "opinion"												
Data													

Excerpts coded with FLAG	Round	Team
Deep Faked podcasts using his voice, similar enough to his topics the make it impossible to deny	1	Orange Pawn
use AI autogenerated communities of fake workers complaining	1	Red Pawn
purchase textbooks that are re-writing history	1	Teal Pawn
grading is out of her control as AI grades assignments	1	Teal Pawn
deep fake videos to change history (like George Washington says) real-time as people bid;	1	Teal Pawn
the anti-democratic party is starting to take power within the USA	1	Teal Pawn
people vote by pop-up ads	1	Teal Pawn
textbook with multi-media, personalized messages	1	Teal Pawn
Deep fake, and automated deep fake generation; I don't need to wait to develop a deep fake compromising YOU, because China a	1	Yellow Pawn
automated distribution capabilities without attribution to China.	1	Yellow Pawn
The Speed of the growth of technology and the unregulated advances in personal computing	2	Black Pawn
Increased social Tribalism	2	Black Pawn
Racial Tensions (nationally)	2	Black Pawn
Educational inefficency leading to increased;	2	Black Pawn
The next technology that we cannot anticpiate/ non state actors/ new political parties	2	Black Pawn
Chinese disinformation campaigns to divide and weaken the US have thus far failed. However, with new policies such as the electo	2	Orange Pawn
Local Feeling /regional priorities	2	Orange Pawn
News Systems	2	Orange Pawn
WOM Campaigns	2	Orange Pawn
Digital communication paltforms	2	Orange Pawn
AI engines scrubbing keywords;	2	Orange Pawn
2000 Bush v Gore - Palm Beach County, Hanging Chads	2	Purple Pawn
2016 Election - Trump mainstreams the concept of Fake News and publicly begins undermining confidence in the impartiality and	2	Purple Pawn
2016 Final Presidential Debate - Clinton asks Trump if he would abide by results of the election; Clinton loses, Democrats begin dis	2	Purple Pawn
Circa 2016 Kanye West aligns himself politically with Donald TrumpTrump appoints Kanye as ambassador to Russia; Dennis Rodma	2	Purple Pawn
Voting goes to online only with fingerprint as identity proof	2	Purple Pawn
2025 Trump formally endorses Kanye as Presidential candidate	2	Purple Pawn
portable genetic engineering tools to splice custom engineered viruses	2	Red Pawn
implanted augments that translate digital info capable of generating physical/psychological effects	2	Red Pawn
IOT hubs at the Edge/ Global IOT protocols	2	Red Pawn
academic/medical research freedom/sharing of research info in non-security communities, freedom of movement/ global quarant	2	Red Pawn
Immersive content getting better,	2	Teal Pawn
Longer battery life enabling extended experience.	2	Teal Pawn
The immersive content industry has legs and there are more than a handful of Pokemon-Go style successes – If Pokemon Go is Fri	2	Teal Pawn
Increased opacity of the algorithms directing people's behavior IRL, and a decrease in corporate desire for transparancy	2	Teal Pawn
Decrease in domestic workforce, increase in off-shore developers with greater responsibility over core business logic and algorithr	2	Teal Pawn
Proxy battles between nation states increase in the information realm – India and China decide to fight it out with information not	2	Teal Pawn
using AI to generate the entire video content;	2	Yellow Pawn
Sylvia got her internship because of an AI-enabled search that selected her from 100,000 candidates of computer science students	2	Yellow Pawn
Internet use/ commerce/credit system is tied to biometric data	2	Yellow Pawn
burner phones illegal	2	Yellow Pawn
highly connected devices are vulnerable to AI attacks to turn on multiple devices in a particular area, capture video/audio, and re-	2	Yellow Pawn
DA in enforcing the law, has to go against public opinion and upset the Family's good rep with citizens	2	Yellow Pawn
Privatizing of public services such as "Goober" (Uber for sustainable and eco-friendly trash pickup)	2	Yellow Pawn
Speed of AI technology - dual use	2	Yellow Pawn
Amount of garbage mob's trash system was picking up is being reduced by environmental impact measures and improvements (i.e	2	Yellow Pawn
Continued acceleration of innovation and technology	3	Black Pawn
Nation State investment and development of reflexive control techniques	3	Black Pawn
Foreign allies and relationships	3	Orange Pawn
Effectiveness of a VR campaign on Soldiers and Allies	3	Orange Pawn
Private sector funded tech with military adoption and possibly infilitation of the supply chain earlier in the process	3	Orange Pawn
Cost of being an early implementer or adopter.	3	Orange Pawn
Where on the adoption curve is the technology we are using for training.;	3	Orange Pawn
Don't have influence over the targets of our enemies	3	Orange Pawn
Mexican government behavior	3	Purple Pawn
Cartel behavior	3	Purple Pawn
The Chinese own and controll the information infrastructure which is leased to Niger. Huwai equipment are used in this infrastruc	3	Red Pawn
Next generation entertainment models powered by 5G, customized by persoan preference models.	3	Red Pawn
Classic man-in-the-middle attack;	3	Red Pawn
Adversary controls the infrastructure - manipulate digital traffic between deployed force and home	3	Red Pawn
Chinese space based systems - what they can see and analyze	3	Red Pawn
The gap between the physical environment boundaries (geography) and boundaryless virtual environment	3	Red Pawn
encrypted networks	3	Red Pawn
Don't have control over local history;	3	Red Pawn
increased domestic terrorism. less lone wolves and more cells (militias, etc).	3	Teal Pawn
continued narrative from the government that they are not as important to fight/combat as international terrorists	3	Teal Pawn
continued interest in mental health apps in lieu of mental health professionals	3	Teal Pawn
above average civil unrest caused by states changing their political parties	3	Teal Pawn
increasing disparities between urban and rural communities as the urban sprawl continues; inflames the division of how the milita	3	Teal Pawn
armed forces behaving badly	3	Teal Pawn
States refusing to send troops to the borders in support of federal policies	3	Yellow Pawn
President has to regain control over Right Coast Revolt; using federal troops is one tool - she has others	3	Yellow Pawn

Excerpts coded with GATE	Round	Team
Government Regulation Restricting Tech to China	2	Black Pawn
Govt Regs ensuring Enhanced Security software embedding technology to succesfully detect deep fakes	2	Black Pawn
companies must demonstrate and certify their due diligence in keeping fake news/deep fakes off their platforms	2	Black Pawn
Fall back planning to include low tech solutions such as paper ballots avail.	2	Black Pawn
"Compute Kill switch" Committee - controlled by a non-partisan, cross-sector, diverse public-private stakeholders.	2	Black Pawn
Platforms for Citizens Engagement	2	Orange Pawn
Acurate Information Dissemination	2	Orange Pawn
Econmic controls and incentives	2	Orange Pawn
Civil Service	2	Orange Pawn
Education	2	Orange Pawn
3, Hacktivists bring down contemporary media streams and interfere with personalized media content to present broader media p	2	Purple Pawn
Institutions of government - military, supporters of traditional constitution and whole of U.S	2	Purple Pawn
Media elite - all formats	2	Purple Pawn
Local Community - strong communities will diminish personalization effects	2	Purple Pawn
Big Tech	2	Purple Pawn
established intelligence network monitoring adversary networks	2	Red Pawn
quantum encryption to defend biodata	2	Red Pawn
redundant security agencies in major transport hubs	2	Red Pawn
quarantine	2	Red Pawn
securitized IOT/global protocols	2	Red Pawn
Corporations tightly control access to and the development of feeds / algorithms, oversight by regulators	2	Teal Pawn
Transparency in the algorithms and operating systems of mobile devices makes it harder to hide malicious code / updates in plain	2	Teal Pawn
Data literacy increases through a function of generational change,	2	Teal Pawn
increased skepticism of social media and extreme online content	2	Teal Pawn
Continue to prevent Chinese + foreign government consumer hardware from gaining traction in the West;	2	Teal Pawn
Manhattan-style project bringing together industry + software experts to regain control of this broken arrow immersive content	2	Teal Pawn
Huawei winning access to the American market;	2	Teal Pawn
burner phones illegal	2	Yellow Pawn
Data privacy law has taken effect which has then subsequently reduced anonymity of data. The legal environment has taken away	2	Yellow Pawn
Loyalty - controls clean sanitation services for the cities which builds good rep with citizens	2	Yellow Pawn
Coming/going of people within trust circles in the family; they can choose who is put in certain areas	2	Yellow Pawn
Need to have access to secure tech that bypasses requirement to tie personal IDs to devices (i.e. biometric spoofing or anonymity	2	Yellow Pawn
National data protection law passed (i.e. pseudo-GDPR) that also requires individuals to be tied to their devices - anonymity reduc	2	Yellow Pawn
Develop AR for DOD Armed Forces (Navy systems) for maintenance of critical weapons systems.	3	Black Pawn
DOD armed services ensure trusted supply chain in defense acquisitions (who is manufacturing the solution, where was it manufca	3	Black Pawn
Develop and invest in technologies to identify Deep Fakes	3	Black Pawn
Security systems within the VR and risk management frameworks	3	Orange Pawn
Social Media filtering for Military and American Families	3	Orange Pawn
Fund studies on the psychological impact of VR tech on human beings	3	Orange Pawn
Dedicated instrusion detection within the VR environment	3	Orange Pawn
Good education for users as well as trainers	3	Orange Pawn
Develop mobile 5G information infrastucture (deployable)	3	Red Pawn
Portable controllable cyberspace	3	Red Pawn
Credential troops to distinguish between fake and real content (audio, video, and narrative)	3	Red Pawn
Authorities to monitor flow over local information infrastructure	3	Red Pawn
Develop the ability to detect 5G mobile ad hoc mesh networks	3	Red Pawn
Signature management - the ability to monitor our own digital exhaust and media output. example Diego post a geo-tagged pictur	3	Red Pawn
Maintain truth and belief in the political process.So, that if a state changes colors - it is accepted as the truth and belief of its citize	3	Teal Pawn
Unify language in the political discourse.unifying American narratives are needed to be crafted and socialized.This would make us	3	Teal Pawn
Passing campaign finance reform.This would support the idea of unifying language by deinsenscentivizing devisive political discour	3	Teal Pawn
Board of medical and mental health doctors that oversee and approve changes to the chatbot.Also need to consider the need for p	3	Teal Pawn
Dont politicize the military	3	Teal Pawn
Providing alternative models for wider segments of the country to participate in defending the nation - serving their country and t	3	Teal Pawn
Rapid acquisition processes to field high-tech to soldiers and increase interoperability	3	Yellow Pawn
Selection of companies who develop tech for military applications	3	Yellow Pawn

Excerpts coded with MILESTONE	Round	Team
Increase Diversity of thought in Govt ,Industryand early childhood education.	2	Black Pawn
Locally important news shared nationally by National News services to provide empathy and understanding across the country to	2	Orange Pawn
Reduciton of the radiciallized national policital news.	2	Orange Pawn
The fear mongering is what other country would like to incite in our country and we are building on and assisting their efforts	2	Orange Pawn
Education on media literacy and data literacy;	2	Orange Pawn
Algorthims to currate the online news and identify and highlight incorrect imformation online	2	Orange Pawn
Digital / online political town halls to discuss and familiar elecotrate with local government	2	Orange Pawn
Evalute digitial participatory governance	2	Orange Pawn
Don't ban the electoral college	2	Orange Pawn
Adapt and adjust to our adversaries' strategies which grow and change as we do.	2	Orange Pawn
Trump loses 2020 re-election bid and peacefully transitions government.	2	Purple Pawn
Convention between big tech and governemnt on ethics in media framing and delivery of ....;	2	Purple Pawn
Enhanced security authentication protocols in addition to biometric, regulate the write privileges of the bio chip (specifics on wha	2	Red Pawn
An effective World Health Organization mediated Treatise	2	Red Pawn
Explore globally banning and penalizing bio-devices that produce physcological effect devices	2	Red Pawn
Credentialing of IoT information sources (accredited media) to counter dis, mis, and malinformation	2	Red Pawn
Hardened augmentation... what is added to your body. Trust, how do we trust these devices? If we can be hit with a bio weapon,	2	Red Pawn
Develop technologies to update and patch the force's augmented (bio) devices from credentialed sources	2	Red Pawn
rapidlyDevelop AI/ML algorithms that analyze and identify anomalies/patterns within open source information indicating the crea	2	Red Pawn
Create a system that protects research institutions IPs;	2	Red Pawn
create a framework for institutions to securely share research information	2	Red Pawn
digital camouflage (can't see you, then they cannot hack you concept)	2	Red Pawn
Develop a tool capable of recognizing modified DNA or genetic modification; example TSA scanner	2	Red Pawn
Discussion of transparency in aglorithms, funding for research of black box algorithm insight – NAS could fund researchers who w	2	Teal Pawn
GDPR-style audting of the algorithm's outputs is more important than its internal workings.	2	Teal Pawn
Expectation that companies are protecting their secret sauce	2	Teal Pawn
Government level support for teams to understand algorithms	2	Teal Pawn
decreased liability for more transparent algorithms	2	Teal Pawn
Investing in research that identifies effective tools and education for increasing digital literacy that can be handled to non-profits	2	Teal Pawn
Digital blue helmets: reserve engineers + scientists + sociologists willing to help foreign nations and other organizations mitigate c	2	Teal Pawn
Former tech executives and engineers end up with public servant roles and have a vastly deeper understanding of how to regulat	2	Teal Pawn
Information warfare geneva convention established, able to identify China and India as violators	2	Teal Pawn
Rapid development in recycling advancements - repurposable recyclables, esp. for 3D printing	2	Yellow Pawn
Rapid improvements in AI that can create entire environments out of scratch, rather than deep faking a face over another actor in	2	Yellow Pawn
Robots capable of separating old electronics increase the profit margin for recycling tech	2	Yellow Pawn
National data protection law passed (i.e. pseudo-GDPR) that also requires individuals to be tied to their devices - anonymity reduc	2	Yellow Pawn
Children's biometric/DNA data can't be legally collected until they are 16. Kids are finding ways to get online without this DNA ver	2	Yellow Pawn
Tech is secretly developed to support the illicit anonymity market.	2	Yellow Pawn
Continued investment in K-12 education (media literacy, critical thinking)	3	Black Pawn
Develop systems, and procedures to verifty and promulgate "ground truth" in crisis situations.In this sceanario, the US sank Japan	3	Black Pawn
Develop security for indivudualized training technologies	3	Orange Pawn
Proactive in adoption standards to ensure tech is at least knew to the hackers	3	Orange Pawn
Better visibility and connection of deployed Soldiers with their families to reduce the target for misinformation and possilbe explo	3	Orange Pawn
Expectation managment of the training benefits of training environments and understanding the potential shortcomings of our se	3	Orange Pawn
Enlist the industry partners to secure the supply chain during early research and adoption	3	Orange Pawn
Norm development with like minded countries to mitigate bad behavior in the information domain	3	Orange Pawn
NIST type standards and regulations for sercurity in the VR environment and design the tools that will help troubleshoot	3	Orange Pawn
Ensure that VR training is considered important training and not considered an afterthough to ensure that Soldiers understand ho	3	Orange Pawn
Need to finds ways to incorporate the cyber and information training pre deployment and ensure clean environments have been	3	Orange Pawn
Establish Central Data clearing house for Operations Research into the Virtual domains and the intergration of training among alli	3	Orange Pawn
Reconcerted effort by U.S. intel community to incorporate human sources to analysis	3	Purple Pawn
Legalize drugs in the US to dry up the market	3	Purple Pawn
Reduce dependence on automated analytics in the IC	3	Purple Pawn
establish grants to support local investigative journalism	3	Purple Pawn
legislate IP protections of articles to mandate attribution and citation, especially for articles that are simply reskinning of existing	3	Purple Pawn
allocate minimum levels of data collection from the field, to validate source inputs and to develop alternative sources	3	Purple Pawn
weigh information used to form findings to ensure outside perspectives are considered	3	Purple Pawn
stress test data for likelihood	3	Purple Pawn
Develop portable, cost effective, deployable 5G communications architecture;	3	Red Pawn
Organic human terrain teams (uniformed)	3	Red Pawn
Electronic warfare capabilities to detect ad hoc 5G networks	3	Red Pawn
AI driven deep fake content detection	3	Red Pawn
Virtualized units whose job is to produce local knowledge; secondarily create a conceirge like service to provide virtualized inform	3	Red Pawn
awareness and monitoring of local services	3	Red Pawn
Augmented reality for MILDEC purposes	3	Red Pawn
deception to quell violent protest; fool satellites	3	Red Pawn
Unbreakable encryption (quantum encryption?)	3	Red Pawn
Enhanced ability to validate networked communications over non-controlled (non-American) information infrastructure.	3	Red Pawn
Blockchaining, ledger technology for validation (non-repudiation).	3	Red Pawn
The accumulated effects of the chatbot result in a severing of the armed force's sense of civic duty – they no longer see citizens as	3	Teal Pawn
regulation of mental therapy apps	3	Teal Pawn
senate pass campaign finance reform	3	Teal Pawn
military work on the narrative of who we are and what we do in order to attract urban individuals, higher income individuals, etc.	3	Teal Pawn
Need to prove that we can handle high-level political dissonance	3	Teal Pawn
can we learn something from how we recovered from Vietnam ... need to see that we can get out of this political era	3	Teal Pawn
Our investments in recruiting new talent to serve and defend our country are so successful that we regain our military advantage	3	Teal Pawn
Trade tariffs	3	Yellow Pawn
data privacy requirements	3	Yellow Pawn
intellectual property requirements have begun bringing tech development back to the US —> leading to slightly increased control	3	Yellow Pawn
Anything to do to address climate change issues	3	Yellow Pawn
Federal gov't no longer subsidizes flood insurance for at-risk locations due to rising coastal waters	3	Yellow Pawn

AI-enabled scanning of networks for intrusions and hacks becomes more common	3	Yellow Pawn
Federal acknowledgement that we did Puerto Rico wrong in the lack of support after Hurricane Maria	3	Yellow Pawn
Education and emphasis on patriotism and national pride	3	Yellow Pawn
Mechanisms (of whatever type...) to increase trust in democratic institutions	3	Yellow Pawn

Excerpts coded with VULNERABILITY	Round	Team
US Citizens are unknowningly participating in Kai Foo Lee's technology and manipulation (physical and biological) - hence rewriting	1	Black Pawn
truth verification	1	Orange Pawn
threatens exsitence of current liberal democracy	1	Purple Pawn
walmarts defenses work at a corporate level; not an individual actor operating outside critical infrastructure - access through her t	1	Red Pawn
people are susceptible to hyper-targetted partisan	1	Teal Pawn
pure human lazyness	1	Teal Pawn
people vote by pop-up ads	1	Teal Pawn
Shame caused by inability to find the people who made deep fakes of her daughter;	1	Yellow Pawn
Value saving her daughter's reputation tied to her duty to country - unless she can nest the two together and the decisive military	1	Yellow Pawn
Election Security	2	Black Pawn
technical vulnerabilities of Social Media	2	Black Pawn
Confidence in democratic insitutions	2	Black Pawn
lack of quality local news in national platform keeps threats at local institution quiet.	2	Orange Pawn
Cultural, social, economic, political, and geographic fissures in the US	2	Purple Pawn
we have a bio chip enabled population with biodata for all citizens; the implanted augments that create positive effects (deeper m	2	Red Pawn
There is no way to determine the physical truth.	2	Teal Pawn
Human vultrabilities in even the most secure technology.	2	Teal Pawn
Indian hackers turn Kaspar by threatening to expose him for his role in the collapse of the Estonian economy. They push him to op	2	Teal Pawn
how unseen/ignored actors influence daily life	2	Yellow Pawn
The viability of fake news	3	Black Pawn
the technical vulnerability of off the shelf products used extensively by the USN.	3	Black Pawn
Also the current tensions between traditional allies in the western Pacific Region	3	Black Pawn
Increased use of AR to perform basic shipboard functions and Fire control	3	Black Pawn
Connected VR systems that are interconnected as well as increased ability for the immersive enviroment to do individual damage t	3	Orange Pawn
Secure encrypted information infrastructure (quantum) preventing a look at what is going on inside Niger. The Brigade's network f	3	Red Pawn
Authorities for capturing local social media data and higher presence on networks.	3	Red Pawn
The risk of politics influencing high level resources within the army such that a commander etc could control or manipulate a chatb	3	Teal Pawn
Undermining trust in digital military network and battle space visualization tools for Military personnel.	3	Yellow Pawn
Undermining social trust in political leadership at local, state and federal levels.	3	Yellow Pawn
Undermining the international trust and agreements between Mexico, US and California.	3	Yellow Pawn

Id	Parent Id	Depth	Title	Description
1		0	Adversary Doctrine Concepts	
2	1	1	Ability to Shape Realities	
3	1	1	Attacks on Critical Values	
4	1	1	Broad Effects	
5	1	1	Control of Media/Message	
6	1	1	Create Mistrust	
7	1	1	Deception	
8	1	1	Disinformation	
9	1	1	Disorganization (distract & create chaos)	
10	1	1	Economic Advantage	
11	1	1	Filter Bubbles	
12	1	1	Incite Violence	
13	1	1	Malinformation	
14	1	1	Manipulation of the Masses	
15	1	1	Micro-targeting	
16	1	1	Misinformation	
17	1	1	Privacy is a Premium Add-on	
18	1	1	Psychological Manipulation	
19	1	1	Radicalization	
20	1	1	Reflexive Control	
21	1	1	Target for Economic Advantage	
22	1	1	Target for Military Advantage	
23	1	1	Target for Political Advantage	
24	1	1	Target the Human as the Weak Link	
25	1	1	Targeting Vulnerable Populations	
26	1	1	Tribalism & Divisiveness	
27	1	1	Truth is a Moving Target	
28		0	Alternative facts become alternative realities	immersive content becomes the only content, yielding ever more real worlds that are based on virtual curation of biases
29		0	Antecedents & Environment Factors	
30	29	1	Algorithms Level the Playing (battle) Field	
31	29	1	Alternate Ways to Receive Information	
32	29	1	Anonymity or Non-attribution	
33	29	1	Attention Economy	
34	29	1	Changes to Democratic Processes & Traditions	
35	29	1	Constant State of Inflammation	
36	29	1	Corporations as Information Tribes	
37	29	1	Decline in Regional/Local News Availability	
38	29	1	Decline of Traditional Journalism	
39	29	1	Difficult to Regulate	
40	29	1	Digital or Social Exhaust	
41	29	1	Dual or Multi-use Technologies	
42	29	1	Fully Connected Data and Sensors	
43	29	1	Human Augmentation Vulnerabilities Exist	
44	29	1	International (Data) Border Porosity	
45	29	1	Internet Provides Anonymity	
46	29	1	No Existing Playbook	
47	29	1	Privacy as a Barrier to Intelligence	
48	29	1	Speed of Narrative Change	
49	29	1	Speed of Technical Change	
50	29	1	Technical Training Required	
51	29	1	Technology Changing Traditional Ways of Life	
52	29	1	Virtual Experiences replace Real-world	
53	29	1	Vocabulary Matters	
54	29	1	Word of Mouth Information Transfer	
55		0	Cultural-emotional hacking	targeting cultural undercurrents as vulnerabilities to be exploited particularly through subconsicous messaging - leading toward one mal-in
56		0	Descriptor Codes	Include categories of FLAG, GATE, MILESTONE, VULNERABILITIES, etc
57	56	1	Flags	
58	56	1	Gates	
59	56	1	Milestones	
60	56	1	Source of Threat	
61	60	2	Business/Corporate Actor	
62	60	2	Political Fundamentalist Actor	
63	60	2	Proxy Actor	
64	60	2	State Actor	
65	60	2	Terrorist Actor	
66	60	2	US Government Actor	
67	56	1	Vulnerabilities	
68		0	Domain Categories	
69	68	1	Cyber Warfare	
70	68	1	Electronic Warfare	
71	68	1	Marketing/Advertising	
72	68	1	Social Media	
73	68	1	Traditional & Social Media	
74		0	Domestic strife leads to international vulnerabilities	an increased splintering of US information sources creates active vulnerabilities for international power grabs
75		0	Elected vigilantes	taking cues from hacktivist campaigns, government enters a new era of social and political manipulation (we tend to elect the "influencers"
76		0	Increased divisiveness creates political localism	with increasing debate and difference, states and local governances believe they are better served as small groups rather than by a nationa
77		0	Information oligarchs & information capitalism	owned information creates an information access divide, particularly surrounding the urban / rural split
78	77	1	Access to Technology Divided by Urban/Rural, Rich/Poor	
79	77	1	Socioeconomic Status	
80		0	Responses or Solutions	
81	80	1	Advertising Must Have Witnesses	

82	80	1	Building Social Understanding								
83	80	1	Data Literacy								
84	80	1	Data Sharing Relationships								
85	80	1	Defense is Costly								
86	80	1	Digital Invisibility								
87	80	1	Digital Participatory Governance								
88	80	1	Global Security Protocols and Processes								
89	80	1	Growth of Emotional Intelligence								
90	80	1	Know-Your-Customer								
91	80	1	Legal or Policy Solutions								
92	80	1	Privatization of Free Speech								
93	80	1	Privitization of National Security								
94	80	1	Reduction of Online Anonymity (technical & policy decisions)								
95	80	1	Reshaping of Institutions								
96	80	1	Responsible & Ethical Uses of AI								
97	80	1	Technical Security Credentialing to Improve Trust								
98	80	1	Thinking Broadly								
99	80	1	Training and Experimentation								
100	80	1	Understand Algorithms via Increased Transparency								
101	80	1	Understanding the Threat								
102	80	1	Use of Quantum Tech								
103	80	1	Verification of News								
104	80	1	When to Break Rules of Data Trust								
105		0	Technical Actions Available								
106	105	1	AI & Machine Learning Used Specifically								
107	105	1	Attack on Critical Infrastructure								
108	105	1	Automated Tools Simplifying IW Ends								
109	105	1	Cyber Attacks (writ large)								
110	105	1	Deep Fakes								
111	105	1	Fake News								
112	105	1	Genetic Data as Source of IW Attacks								
113	105	1	Geo-fencing Technologies								
114	105	1	Multi-platform Amplification								
115	105	1	People Vote by Pop-up Ads								
116	105	1	Spoofing								
117	105	1	Use Insider Access								
118	105	1	Use of Big Data Sets								
119		0	Who Is Affected?								
120	119	1	America's Economic Gaps								
121	119	1	America's Education Gap								
122	119	1	Creating Problems that Don't Exist								
123	119	1	Cross-over Effects (i.e. US to EU)								
124	119	1	Fragmentation of Our Personal Realities								
125	119	1	Fringe Players Have a Voice								
126	119	1	How do We Know What to Trust?								
127	119	1	Impersonalized (electronic) Relationships								
128	119	1	Let a Computer Make Decisions for Humans								
129	119	1	Moving the Goalposts of Achievement								
130	119	1	One-to-one Relationships								
131	119	1	People are Judging You Silently								
132	119	1	Saving Reputation as a Lever								
133	119	1	Shame as a Lever								
134	119	1	The Digitally Addicted								
135	119	1	Turning People Into Product								

Post Analysis Workbooks

(Third Workshop)

Round	Team	Round One - "Summary"	initial codes
1	G1B1	A battle for truth. Struggle to influence the information environment to our advantage. We can't control it, so how do we leverage it to our advantage while maintaining our American ideals, they are being used against us. The two ends of the spectrum, feedom and control. Adversaries leveraging our freedoms against us and then highlighting our controls as hyprcracies. Stating our controls violate our own principles. Is it freedom of speech if we deny access or sensor. (G) Have to have the capability to insert our narratives into any system, at any time. (G) Authorities to act, respond, and deploy information capabilities. (G) Government regulation of information dissemination platforms. (G) Analyze, monitor, and influence the private data of foreign national's data to de-legitimize adversarial information. (G) The ability to conduct CNA, CND, and CNE on adversarial controlled information	battle for truth; freedom vs control; manipulating the narrative; humans as sensors; recognizing deep fakes; reactive strategies; words that mobilize action
1	G2B1	China has positioned itself to control and influence the economic, information and diplomatic environment in order to achieve desireable conditions without the use of overt military presence, specifically the ability to generate plausible narratives and target individuals. Lack of priority given to there integratation of the physical, informational, and cognitive domains by failing to seize and retain the initiative. Dual-use ICT systems manipulated by hostile actors, constraining friendly actions to affect that system. Lack of diplomatic cadre, a reduced number of FSO, lack of global efforts. Lack of competing economic influence and ties within country. (G) Risk aversion and authorities restrain the ability to execute IRCs. This must be addressed through policy and military culture. (G) Difficulty and legal challenges to training in the IRCs; specifically EW, CO, MILDEC, CMO, and MISO. Address	tech advancement is economically hinged; non-US IT products restrict our access; Cyberspace & IW operation models; microtargeting continues
1	G3B1	The adversary owns the inftrastucture and is the communications is across all domains, in both the operational environment as well as the homefont. Continual engagement with the information environment. Reliance on 5G network for communication creates opportunities to exploit vulnerabilities and attack network credibility. If the Chinese and proxy forces are primarily using the communication network as an attack vector, the US can disrupt this and degrade their capability to message. Furthermore, degrading the network within the Chinese border and preventing internet access to their population could sow distrust with the Chinese government. "Exposes a tactic technique or procedure that that can be used by any entity. Vulnerability for China, because the US can do the same actions against China. US can fuel unrest and motivate the population to oppose the	dual-use technology dependencies; changing the US image to the world; words that mobilize action; IW training requirements;
1	G4B1	China has had the ability to get proactive in operating enviorment vs our reactionary response. The chinese capabiltity to conduct reflexive control and US lack of capability/willingness to employ reflexive control at the unit level. The sheer number of people china can throw at a problem vs us capability. (G) BCT capability to monitor digital pattern of life in local area (In the S2). (G) Culture change within the combat fighting force to see information maneuver as a critical piece of maneuver. (G) Resource control over rare earths, raw materials. (G) Can American government influence media companies creating narratives that are contrary to american interests or supporting chinese narratives. (G) Chinese financial influence in American institutions. (G) Anti-Chinese messaging by American media institutions. (G) Domestic messaging tied to actual socio economic status to improve under	reactive strategies; using tech to overcome human shortfalls; intertwined colonial influences; humans as sensors; tech advancement is economically hinged; Cyberspace & IW operation models
2	G1B2	Wedging - creating conflict between groups working in solidarity. The ability for adversaries to manipulate or create conflict from culturally different groups through virtual manipulation. (G) Regulation, policy, law, and strategy that enhances the positive uses of technologies and diminishes its negative effects. (G) The acquisition and use of technology to include foreign national data - AI/ML training. (G) The ability to monitor and analyze data flowing across USG networks and devices; control military members use of personal IoT devices. (G) Ability to access, exploit, or attack adversarial controlled networks within the cyber domain. (G) Conduct physical engagements with allies and partnered groups as a method of validation. (G) Public service announcements that raises awareness of these possibilities. (G) Acquisition of technologies and where those technologies are manufactured. (F)	wedging virtually (using IE for advantage); freedom vs control; face to face validation of virtualized information; proof of social media manipulation;
2	G2B2	Adversary has broad based persistence access to information presented to the military in both official and unofficial means in order to create weaknesses between forces. Cultural manipulation, by exploiting views on privacy. Attack vectors are small of in scale and impact not an immediate threat, but culminating effect could achieve a major effect. (G) Promulgation of Information enviornment conditions and standards to report abnormalities. (G) Build positive enviornment through IO campaign on own forces. (G) Planning and encouraging social engagement. (G) Real time analysis of our own social media footprint. (G) Map and analyze military members who are vulnerable to manipulation or exploitation - OPM, Posts. (F) Abnormal cell and social media behavior. (F) Insider threat behavior. (F) Adversary media outlets developing narrative counter to reality, supporting their IO campaign. (M4)	cultural manipulation; identification of government "digital exhaust"; IW training requirements; proof of social media manipulation
2	G3B2	INDIVUALIZED personally attacks through personal network devices as well as AR/VR training devices as a micro deception effort. Risk for exploiting personal vulnerabilites exposed thorugh individual networked devices. (G) Acquisitions process to develop network devices- built in resiliency and encryption to deter attack- hardware and software. (G) Education & innoculation of Soldiers and their families to current adversary TTPs throughout competition- we operate in a disinformation environment. (G) "Improve ""Virtual"" integration with partners and develop TTPs and lesson's learned early and often. Maintain personal relationships to defeat an adversary's virtually implanted disruptions. (G) Enhance people's capability to build personal trust through physical interaction. Enhanced social skills to build trust. (G) Work with social media and media platforms to improve authentification and	proof of social media manipulation; microtargeting individuals; non-US IT products restrict our access; dual-use technology dependency; using tech to overcome human capital shortfall
2	G4B2	Micro targeting of the persuadables and using old school targeting techniques in a new avenue attack. We're more vulnerable to cold war tactics of reflexive control that are faster and more interconnected than under the cold war. the inabilty to agree that the russians are our enemies enables their continued freedom of maneuver. The adversary has the ability to get inside of our social decision making cycle. (G) limit advertising/targeting data gathering on military, government, and family members. (G) develop and use bot networks to create defensive social media networks. (G) continuous media messaging to increase the awareness of the force and their families of dis/misinformation. (G) what are the limits of surveilance capitalism and what are the limits of what companies can do with this? (G) Long term conditioning of digital skepticsm within population. (G) periodic assessments of	changing the US image to the world; deep fake recognition; cultural manipulation; identification of government "digital exhaust"; freedom vs control; IW training requirements
3			
3			
3			

	Round	Team	Round Two - "Meaning" / "Insight"	Round Three - "Novelty"	Discussion
	1	G1B1	leveraging info environ to maintain American ideals; complete control of IE is impossible (and likely not an American ideal anyway); adversaries are unscrupulous in manipulating information (i.e. lying is the norm, but may not be an American ideal); in the battle for truth, will highlighting adversarial injustices move the	American ideals are not equally sought after around the world; the 2030 US brand relies heavily on the 1950 US brand --> is this still desirable to the world? What role does the military play in that brand?	"Insert[ing] our narratives into any system, at any time" is a wide exclamation of hubris. This relies on the principles of democratic theory, meaning that the US/western way of life is superior to other ways of life & government because we have a democratic governance model. --> This also implies that our intelligence and cyber operations are fully connected into EVERY system. Is that possible in the future of consumer-level AI? So if we want to be able to "insert our narratives" into another system, it better not be in English and it better be culturally nuanced and savvy of how those IN the system like to receive their narrative. This is an overwhelming challenge for the DoD whose cultural feeder systems do not value multi-lingual and multi-cultural learning --> there are also at least 4 major difficult languages/cultures to become expert in, whereas our adversaries only need to learn English and watch pop culture to understand us. Russia and China have strategies to balkanize and isolate their information flows (textbooks & great Firewall in China and RuNet in Russia). --> Have the drivers of US influence (democratic & capitalistic values) in the
	1	G2B1	China's soft power comes from economic incentives and improving tech sales & installation; too few people to verify events face-to-face (trust diminished when tech is only contact with others); deep fake recognition technologies are essential	tech is shiny and allows for reduced people/risk, but people are better at verifying truth; future of conflict will be informational, yet governing strategies remain physical; beating China's soft power approach requires competitive alternatives to Chinese products	
	1	G3B1	control over the communication network may be a viable alternative to controlling the narrative; exposing Chinese skeletons in the closet may pressure their government from within; building the US brand for the 2030s is different than for the 1950s; education of the population about IW possibilities/threats	US needs to fight back, but we may not need to fight dirty; exposing Chinese atrocities at home & their reliance on compromised tech for surveillance purposes is a knife that cuts both ways;	
	1	G4B1	Chinese "long war" strategy vs US cyclical & rapid gains mentality; mass entertainment to share correct ideals; enabling African self-actualization (i.e. dry up need for Chinese products)	investing in a patient, long-term strategy is essential to keeping on par with Chinese political/economic expansion	
	2	G1B2	face to face validation of relationships and virtualized information; service members and family members are global digital citizens --> spend resources evaluating and educating on the strengths/risks of common digital products that they use;	evidence of social media manipulation is essential for understanding better truths	How does the DoD respond to the balance of protecting its own by implementing regulations, training, specialized and isolated information networks with the overload of information available outside these proposed enclaves? Control is much tighter inside the DoD information space, at the risk of shielding our service members and families from alternate points of view contrary to DoD policy; alternately, there is no way to implement full controls on social media. A concerted government effort to convince the social media companies to filter content (e.g. fake and inflammatory) must also fight against a economic incentives to have an open platform as well balance freedom of speech and privacy concerns at the same time. --> techniques to show proof of social media manipulation might convince savvy populations, but those suffering from a confirmation bias (i.e. flat-earthers, etc) will ignore external sources of proof.
	2	G2B2	monitoring our own (for vulnerabilities to exploitation) and perhaps controlling our military "digital exhaust" is desireable yet maybe unmanageable	"society" and "culture" are often considered singular entities in military planning --> they aren't...;	
	2	G3B2	individualized attacks are high reward --> make them high risk, too (face to face relationships, monitor high profile/high risk people with "digital guard dog" programs); automated OPSEC monitoring tools	tech tools for simplifying certain tasks, but human eyes to validate certain truths --> still runs the risk of human cognitive vulnerabilities, but until we get AI tech good enough to filter the difference we need 2-factor validation (tech & human)	
	2	G4B2	disruption (with no other ends) is a viable strategy --> used by Russians; we must understand the values & ideals of the companies providing social media services, because these values are the only form of control the US can impose on speech	military strategies of disruption and delay are not often seen as favorable, but what the US may need is simply time for governance, research, and values to catch up with the speed of tech --> make disruption & delay primary IW strategies	
*	3				
	3				
	3				

Excerpts coded with GATE	Round	Team
BCT capability to monitor digital pattern of life in local area (In the S2).		
Culture change within the combat fighting force to see information maneuver as a critical piece of maneuver.		
Resource control over rare earths, raw materials.		
Can American government influence media companies creating narratives that are contrary to american interests or supporting chinese narratives.		
Chinese financial influence in American institutions.		
Anti-Chinese messaging by American media institutions.		
Domestic messaging tied to actual socio economic status to improve under served American regions to stimulate support for foreign partner investments.		
Regulation, policy, law, and strategy that enhances the positive uses of technologies and diminishes its negative effects.		
The acquisition and use of technology to include foreign national data - AI/ML training.		
The ability to monitor and analyze data flowing across USG networks and devices; control military members use of personal IoT devices.		
Ability to access, exploit, or attack adversarial controlled networks within the cyber domain.		
Conduct physical engagements with allies and partnered groups as a method of validation		
Public service announcements that raises awareness of these possibilities.		
Acquisition of technologies and where those technologies are manufactured.		
Risk aversion and authorities restrain the ability to execute IRCs. This must be addressed through policy and military culture.		
Difficulty and legal challenges to training in the IRCs; specifically EW, CO, MILDEC, CMO, and MISO. Address this concern through DOTMILPF and policy/regulation.		
Work to preclude and counter the distribution and employment of ICT from malicious actors. Offer competitive solutions developed by friendly nations.		
Diplomatic efforts to build up the image of UN/ Foreign forces prior to and during the deployment, build relations with population.		
Maintain and increase interaction with host nation and local populace through various agencies and at multiple echelons of government.		
limit advertising/targeting data gathering on military, government, and family members.		
develop and use bot networks to create defensive social media networks.		
continuous media messaging to increase the awareness of the force and their families of dis/misinformation.		
what are the limits of surveilance capitalism and what are the limits of what companies can do with this?		
Long term conditioning of digital skeptiscm within population.		
periodic assessments of social relationships with partner nations forces (METT-C dependent).		
actions to identify vulnerable members of the population.		
identify national loyalty that may be higher among immigrant pop vs native born.		
Acquisitions process to develop network devices- built in resiliency and encryption to deter attack- hardware and software.		
Education & innoculation of Soldiers and their families to current adversary TTPs throughout competition- we operate in a disinformation environment.		
"Improve ""Virtual"" integration with partners and develop TTPs and lesson's learned early and often. Maintain personal relationships to defeat an adversary's virtually implanted disruptions.		
Enhance people's capability to build personal trust through physical interaction. Enhanced social skills to build trust.		
Work with social media and media platforms to improve authentification and security of current commerical platforms that Soldier's use.		
Prepare to use same methods to attack the adversay and demonstrate our capability. Punish them for their actions by doing the same as a way to deter future attacks.		
Promulgation of Information enviornment conditions and standards to report abnormalities		
Build positive enviornment through IO campaign on own forces.		
Planning and encouraging social engagement.		
Real time analysis of our own social media footprint.		
Map and analyze military members who are vulnerable to manipulation or exploitation - OPM, Posts.		
Have to have the capability to insert our narratives into any system, at any time		
Authorities to act, respond, and deploy information capabilities.		
Government regulation of information dissemination platforms		
Analyze, monitor, and influence the private data of foreign national's data to de-legitimize adversarial information		
The ability to conduct CNA, CND, and CNE on adversarial controlled information infrastructure		
Humans as sensors using police tactics as example. Legally they cannot collect, but they can sense.		
Provide an alternative invastrudture for developing country - US initiative but acccomplished by Industry.		
Reward information savy and exceptional soldiers/officers.		
Find a way to bring the information environment into the training environment. If we see and practice, one can integrate and reward.		
Developing units to provide the information capability to units that are already overloaded with current tasks to become experts across the current domains.		
Leader education and development.		
Actions within communities of the Chinese to message to the US.		
Create same offensive capability and use against adversary to deter future operations. Would not need to lie since adversary commits crimes/atrocities as regular practice.		

Excerpts coded with FLAG
foreign digital reliance on chinese networks.
chinese control over natural resources; population information control.
Sino-African future population due to population interbreeding- where is the loyalty.
Black market that operates outside of chinese social credit system- what does this look like - is it digitally segregated or analog?
Chinese whole of nation approach vs US separation between political and economic agencies/institutions.
Chinese force projection capabilties - what is their force presence/capabiltities outside of mainland china.
Allies and strategic partners networks, network devices, or the controls they emplace for the use of these technologies.
Unethical use of technologies in novel ways; troll farms, deep fake content production (disinformation).
Adversary network, network devices, or the controls they emplace for the use of these technologies
Service member's family's network, network devices, or private data.
The creation and managment of foreign social media applications.
No viable alternatives to Chinese owned ICT providers in Africa
Evidence of successful low level deep fake attempts, integrated into the operating environment.
China or threat is able to gain economic control in host nation, with long term infastructre and assets.
As nondiscretionary spending requirements increase for the US, the DOD faces reductions in funding.
Reduction in funding and manning for the DOS and other diplimatic engagement tools.
Growth in pro- Chinese messaging in the local environment, IE observation of China shaping the environment.
Inroads made by a Chinese version of Russia Today.
we can't control what social media people are on
what are the free speech limits that the government can impose on media/data companies?
Legal/regulatory limitations on data operations within US/targeted to US Citizens.
by ignoring lack of shared understanding of virtues and vices.
Ability of Natural Language Processing to map to regional and cultural dialects. Elimination of cultural clues and errors in speech.
Increase of non-discriminate targeting of families / soldiers.
Increase of discriminate targeting of families / soldiers.
Increase of adversarial deception operations through social media and tech applications.
Adversary's collect and attack units and leaders at the tactical level (Interest by adversaries at lower level of org chart).
Abnormal cell and social media behavior.
Insider threat behavior.
Adversary media outlets developing narrative counter to reality, supporting their IO campaign.
Development of AI/ML - unconstrained access to global data
We don't have control over words and concepts in cyberspace until people, societies, populations act on those worlds. However, our adversaries can.
Motivation for influence (OROB - "one road one belt") - national debt due and consequences - implications, such as Venezuela
A nation's partner of choice - China outspends us and Russia out arms - example China lends for infrastructure and then uses is own labor over local.
Space and their ability to control ground level perspective - counter space.
Expansive of the great fire wall to include nations they put information infrastructure into - expansion of social
China willing to use proxy forces /provide information to lethally attack US forces.
Global expansion of Chinese owned networks.
Reliance upon Chinese owned networks by 2nd/3rd world countries.
Early creations of deep fake content.
How does China deal with current "information warfare"- i.e. Hong Kong. This will indicate future techniques, tactics, and procedures.

Excerpts coded with MILESTONE	Round	Team
Whole of government approach identifying China as primary adversary on DIME and policies that support local infrastructure.		
Forward deploy US forces to develop strategic partnerships across Africa (establish an infratructure foothold that enables information foothold)		
Establish gov't investment in food and water security (desalinization) that enables local governance and self sustainment/energy in Africa to build local trust to counter the information narrative.		
Develop capability and capacity to conduct "information maneuver" tactically.		
Phase AFRICOM to be physically located in Africa.		
Develop military/economic/information relationships with African Union.		
Target mass entertainment media environment to leverage emerging African entertainment/consumer markets.		
Long term resource security focused on self actualization/self determining to avoid colonialism associations.		
Acquire data set necessary for training AI/ML to identify and learn recognizable patterns of social media manipulation.		
Create incentives for companies/corporations to manufacture networked technologies within U.S. regulations for these devices. To include the mining of the semi-precious metals used to create these devices (anti-hardware hacking).		
Increase the protection of intellectual property and the regulation of the devices used by service members abroad.		
Educate service member's family on the necessity of validating information acquired through social media, solely dedicated to the families of deployed service members. Establish a Military contact agency dedicated to validating this information.		
Establish physical engagement and validation protocols as a response measure to reported incidents of social media manipulation affecting strategic partner relationships.		
Develop an AI-driven persistent virtual force that monitors for patterns of social media manipulation; learns of adaptive techniques; and identifies sources of social media manipulation. [Whole of government].		
Include the necessity of coalition social media manipulation task forces within Status of Forces Agreements. [State Dept., DoD].		
CPOE/EW in order to preapre to degrade, disrupt, or subvert dual-use ICT in the event of its weaponization.		
Indoctrinate Information Warfare into military training programs.		
Develop and promolgate counter deep fake tech and knowledge. [industry/ Cybercom].		
Increase of diplomatic and economic participation in vulnerable host countries. [State / private industry].		
Prepare and maintain guerilla forces with complementary information warfare cells and training.		
Traditional manuever warfare is executed suborinate to grand strategy narratives via cooridnated information warfare.		
Install either aligned or neutral networks in vulnerable host countries, via cheaper networks (google blimps). [Western Industry].		
Secure/Protected communications capability for soldier use to replace civilian technology dependence. [Google, SpaceX, etc].		
Establish and conduct sensitive Title-50 activities with sympathetic populations.		
US strategy should have Redlines, and actually defend them, enhance credibility.		
Messaging and Deterence actions through cyber means to known cyber threats.		
AFN messaging on Russian Infuence Operations.		
Improved IA training to discuss threats in Social Media and adversarial influence operations		
Develop resilient tech.		
Educate forces and families.		
Build pretected family/military social media network within an established framework (Facebook with a .fam.mil access only) that is firewalled off.		
Government/Industry collaboration to protect privacy.		
AI development to collect information on open-source platfroms to build org charts / order of battle to understand who potential individual targets are.		
Artificial Intelligence Units that manage the entire environment to assist in the truth.		
Win the AI "space race".		
Integrate a WEB Opsec cell into the Corps' I2CEWS/ Information Warfare Capability in order to provide continuous protection. [Regionally Aligned Combat Commands].		
Monitoring or Fraud system for social media. [Industry].		
Legal authorities to protect and defend all information pertinent to military objectives to inlude private social media interaction by active service members. [congress].		
Enforce human interaction. [DOD/DOS].		
Conduct intrusive IW campaign against adversary, use messageing against and take down capability. [DOD, CYBERCOM].		
Modelling of manipulation for own force, continual measurement of vulnerability. [OPM, FBI, DOD].		
Monitoring and protection for SM family social media footprint.		
Maintain IO training.		
Maintain deterrent IW Campaign, to keep adversary on edge		
Highlight adversarial vulnerabilites through narrative - oppression of minorities, indebting of non-industrialized nations. [National information agency, such as an enhanced GEC or re-constituted USIA].		
Stop exasperating our own issues - producing narratives that disparage ourselves - poor job of mitigating our own issues. [Whole nation].		
How do we need to train our soldiers for response to deep-fake at the tactical level; Cultural awareness; use the SOF models; focus on relevant training - 350-1 distraction; Field time - more time spent practicing our skill craft. [TRADOC].		
Soldiers as technologically enhanced soldiers - cameras, recording devices to capture what occurring in the field.		
We need to have the capability to identify the deep-fakes and state why its fake, how they created it; Social component - sell it to legitimate media sources - sources world views as reputable for truth telling. [Army, DoD, USG].		
Congress and senior leaders of the DoD to be willing to accept more risk - youth. [Congress - DoD senior leaders].		
Use of available data sets for training AI/ML algorithms - if we don't and our advesaries do, are placing ourselves at risk. [Congress, DoD,].		
Counter space technologies - ability to protect our assets and defeat theirs. [DoD, Space Command].		
More willing to use classified capabilities (cyber,space based) at the tactical level. [DoD].		
Stop overclassifying capabilities - Snowden tools are within the open-source space; however, classification forbids us using these tools at the tactical level; our adversaries are using our own tax payer funded tools against us...		
Understand how to exploit the Chinese/adversary networks.		
Professionalize an 'information domain' force. This could be a top-down process or bottom-up development.		
Capability overlap- information maneuvar does not belong to just one unit. All maneuvar units deal with information warfare from infantry to cyber to SOF, etc.		
Military/Industry collaboration to innovate new concepts/technology to counter the threat.		
Cultural/organizational changes to recruit the best fit persons to fill cyber/information jobs. Can the military take advantage of a "privatized cyber/information army".		
Exploit population grievances within the Chinese population.		
Continue to respond to humanitarian crisis in order to establish and maintain US credibility. This will sway populations in the US favor when they must decide between a US narrative vs. an adversary's narrative.		
Gain access to Chinese built networks both inside China and inside Chinese-supported nations.		
Need to develop our brand, and one that will sell itself and assure that the US/Allies are the best offer for mankind, not just the US.		
Inoculate the population and education them against the issues in the Information Age.		
Educate the population on real vs fake- institutionalize critical thinking.		
Education on the understanding of the new invastion. The economic invasion of the world by Chinese.		
Develop a "encryted tag" to media to prove validity of digital media. Tags will be given to 'vetted' reporters. This will help diminish the credibility of deep fake media that is injected into social media (if it is missing a tag).