INFORMATION DISORDER MACHINES

WEAPONIZING NARRATIVE AND THE FUTURE OF THE UNITED STATES OF AMERICA

A Threatcasting Lab Report

INFORMATION DISORDER MACHINES

WEAPONIZING NARRATIVE AND
THE FUTURE OF THE UNITED STATES OF AMERICA

INFORMATION DISORDER MACHINES

WEAPONIZING NARRATIVE AND THE FUTURE OF THE UNITED STATES OF AMERICA

Technical Report by Brian David Johnson
From 2019 Threatcasting Workshop hosted at
Arizona State University produced by Cyndi Coon.

The Threatcasting Lab is supported by

When I created the threatcasting process the intent was not only to envision possible threats but to empower people and organizations to take action. The Threatcasting Lab at Arizona State University's charter is to empower by bringing together people and organizations to collaborate and using the output of the lab to create tools that help make organizations and people safer in the future.

- Brian David Johnson
  Director Threatcasting Lab

Table of Contents

10 Participants and ASU Threatcasting Lab Team
12 Executive Summary
14 Threatcasting: A Brief Overview
16 Introduction
18 Threatcasting Workshop Goals
20 Threats: Information Disorder
22 Threat Future 1: *There will be Blood*
23 Threat Future 2: *New Texas Rising*
24 Threats: Information Disorder Machines
26 Adversary: A Failure of Vocabulary
28 Threat Future 3: *The Worst of Ourselves*
29 Threat Future 4: *A Family Affair*
30 The Worst of Ourselves: Ourselves Against Ourselves
32 Business Proxies
32 Weaponizing Authenticity
33 Catastrophes as Amplifiers
34 Threat Future 5: The Authenticity Revolution
36 Implications and Actions
38 Flags: External Indicators
40 Actions
42 Further Analysis of Weaponizing Authenticity
44 Appendix

Participants

Jason C. Brown	Arizona State University
Nitin Agarwal	Collaboratorium for Social Media and Online Behavioral Studies (COSMOS), University of Arkansas - Little Rock
Brad Allenby	President's Professor of Engineering, Lincoln Professor of Engineering and Ethics, Arizona State University
Matt Chessen	
Joel Garreau	Weaponized Narrative Initiative
John F. Gray	Mentionmapp Analytics Inc.
Alec Guthrie	
Andrew O. Hall	Army Cyber Institute
A. Kavanaugh	
Toby Kohlenberg	Dropbox
Samuel Krivin	Weaponized Narrative Initiative
Marvin Leal	
Rhiannon Leal	
Diego Fregolent-Mendes de Oliveira	The Rensselaer Polytechnic Institute & US Army Research Laboratory
David M. Perlman	Ph.D., CoPsyCon
James Prince	The Democracy Council
Kristy Roschke	Arizona State University
Robert James Ross	Ph.D., Army Cyber Institute
Scott Ruston	Arizona State University
Kurt Sanger	US Marine Corps
Lisa Kay Solomon	
Lucille M. Tournas	Arizona State University, SOLS
Christopher R Walker	Marvelous AI

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.

Information Disorder Machines

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 micro-targeting 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.

Threat Futures:

- 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.

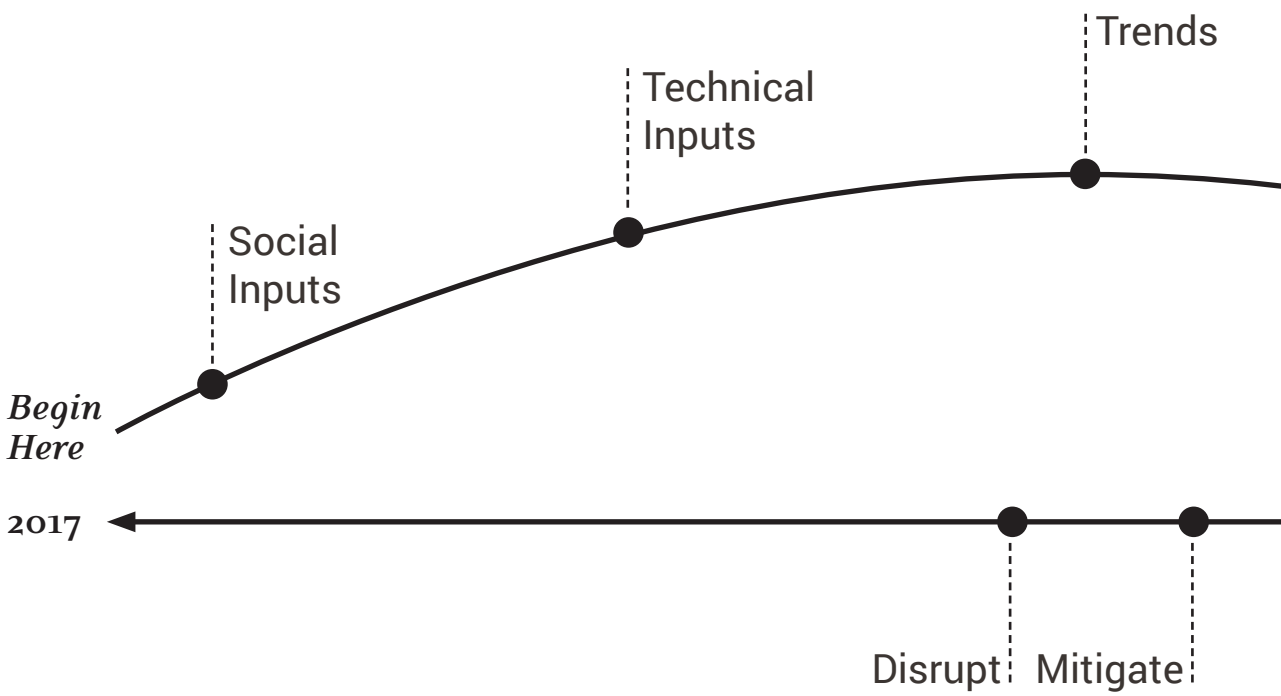
The Threatcasting Workshop also identified a range of possible ways to disrupt, mitigate, and recover from the threat of IDMs. These actions span across multiple domains including government, military, industry, trade associations, academia, and average citizens. A single organization can not meet the 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.

Threatcasting
A Brief Overview

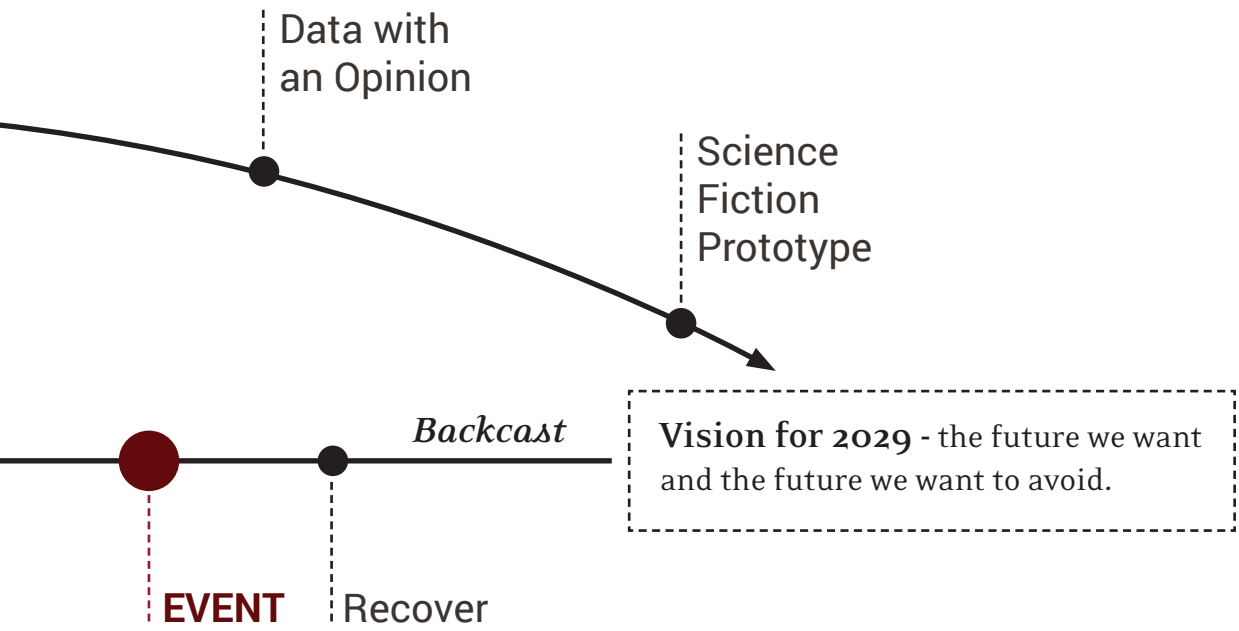
Threatcasting is a conceptual framework and process (see Figure below) that enables multidisciplinary groups to envision and plan systematically against threats ten years in the future. Groups explore how to transform the future they desire into reality while avoiding an undesired future. *The threatcasting process is described in detail in Appendix 1.*

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 fiction story, it allows readers to imagine what needs to be done today and then three 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 important. Diversity of age, experience, and education within small groups are key but tied to a common thread - they are 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 are from academia, private industry, government, and the military.



Introduction

"Weaponized narrative is an attack that seeks to undermine an opponent's civilization, identity, and will. By generating confusion, complexity, and political and social schisms, it confounds response on the part of the defender."

A fast-moving information deluge is an ideal environment for this kind of adversarial attack. A firehose of narrative attacks gives the targeted populace little time to process and evaluate. It is cognitively disorienting and confusing – especially if the opponents barely realize what's occurring. Opportunities abound for emotional manipulation undermining the opponent's will to resist.

The following report captures the goals, subject matter expert inputs, raw data, and findings of Arizona State University's Threatcasting Lab Workshop exploring the future of Weaponized Narrative. The findings exposed multiple threat areas and the coming of information disorder machines (IDMs) that could harm individuals, organizations, and even the entire United States of America. To empower people and organizations to disrupt, mitigate and recover from these potential threats the findings in this report identify not only specific threats but also provide recommendations through which organizations and individuals can disrupt, mitigate, and recover from the future of effects of IDMs.

Threatcasting Workshop Goals

The Weaponizing Narrative Threatcasting Workshop is intended to assist broader communities with envisioning future threats and vulnerabilities made increasingly more complex by rapidly evolving information technologies and weaponized narratives designed to sow chaos and polarization among targeted populations. America's adversaries in the world realize that currently, they cannot defeat us in a head-to-head military conflict, so they will rely heavily on attacking America's institutions, and the values that hold them up even before war has begun.

Adversarial methods use the combination of weaponized narratives, the susceptibility of Western ideals, and historical divisions that exist between groups within societies to achieve their diplomatic and strategic aims. These methods allow adversaries to deny attribution for false narratives or may use covert military activities designed to deceive.

Future information technologies, such as AI-enabled algorithms that can automatically generate narratives, are going to speed up the abilities of adversaries to influence targeted populations and get them to act in a manner that is advantageous to the adversary.

How can the United States imagine and bring together the resources across multiple domains that will be capable of supporting a national-level strategy for competing in the future information environment?

Using the Threatcasting process Arizona State University's Threatcasting Lab convened over 40 practitioners together for two days on the campus of ASU in Tempe, AZ to explore possible and potential threats futures based on subject matter expert inputs (see appendix).

The group developed 24 threat futures (see appendix) that formed the basis of raw data that has been analyzed for the results of this report.

Information Disorder

For the Threatcasting Workshop, we explored the future of Weaponized Narrative by using the term and concept of "information disorder." This term was coined in a 2017 Council of Europe Report, "Information Disorder: Toward an interdisciplinary framework for research and policymaking" by Dr. Claire Wardle and Hossein Derakhshan. The report introduces information disorder in this way:

"We, therefore, introduce a new conceptual framework for examining information disorder, Identifying the three different types: mis-, dis- and mal-information. Using the dimensions of harm and falseness, we describe the differences between these three types of information:

Mis-information is when false information is shared, but no harm is meant.

Dis-information is when false information is knowingly shared to cause harm.

Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere."

Functionally, the concept of information disorder provides a means to capture, understand, and specify the types of narratives and how they are being used.

Recently, building off Information Disorder (DES) Ben Decker explored the concept of Adversarial Narratives. "Intentionally distributed narratives that seek to enrage and divide Internet users without a required chronology or sequence of web artifacts can be defined as adversarial narratives. To further flesh out that definition, we can understand adversarial narratives as narratives rooted in, involving, or strongly characterized by conflict or opposition between actors and their interests, and especially between a social in-group and an out-group. Adversarial narratives can be identified by key characteristics within the contents and meaning of web artifacts, as well as how they are distributed. When these types of adversarial narratives are deployed, they create a series of smaller conflicts among asymmetric actors.

For our discussion, an adversarial narrative creates a networked conflict, in that it takes place at least partially over electronic communications networks, employing the tools and functionality of those systems to influence other actors' behavior and linked outcomes, and which may result in harms or setbacks to the interests of one party. By describing this paradigm as a conflict, instead of war, our definition can include a broader range of hybrid threat agents, including state actors, private influence operators, grassroots trolls, and pure rent-seekers. Motivations can organize them (from political to financial) and degree of structure (from highly centralized to decentralized), yet they all abuse and exploit adversarial narratives across the web ecosystem.

Adversarial narratives are effective because they inflame social tensions by exploiting and amplifying perceived grievances of individuals, groups, and institutions. The term itself is agnostic to the truth-value of the messaging contained. This is an important distinction to make because... there are kernels of factual legitimacy located throughout the narrative. It is only later on, once the narrative begins to travel upstream, do the fabricated conspiracy elements come into play."

Information disorder provides a means to capture, understand, and specify the types of narratives and how they are being used.

There will be Blood

November 2028. San Antonio, TX

The video shocked Tammy, enraged her into action. The socialists had gone too far...they were now deputizing illegal immigrants, confiscating gun owners property and using it to "protect" polling stations...they were rigging the election...denying people their right to vote. Tammy grabbed her AR-15 and decided to do something about it...

The video shocked Diego, enraged him into action. The alt-right militias were beating up women of color, not allowing them to enter the polling station to vote...accusing them of being illegals and handing them over to ICE. Diego grabbed a bat and decided to do something about it...

Tensions at the polling station continued to rise as more people arrived...both sides screamed accusations.

Tensions at the polling station continued to rise as more people arrived...both sides screamed accusations... neither would back down. The election and democracy was at stake.

Then the pushing started... someone got hit in the face... another was pushed to the ground...a man rushed at Tammy with a bat...she jumped back, pulled the trigger...Diego collapsed... blood pouring from his chest. The violence continued...

Three months later...after the funerals and trials... both videos were revealed to be fakes, shared by foreign state-backed social media influences on both sides...but by then nobody believed it or cared...the election was rigged...

(Blue Chip 2)

New Texas Rising

2029. Dallas, TX

A decade ago nobody thought Texas could leave the United States...now they were just one referendum away. Walking away from the voting station, Pablo checked the latest poll numbers...Stay 42% Leave 43%... Then he saw the message that Star Direct Power, his last remaining client at his law firm, was dropping him because he wasn't "Nex Texas" enough...

Pablo couldn't look away from his video news feed...Militia Violence at the Border... Alt-Right Fraud Found in 2028 election - New Investigation Pending...Secret Federal Government plot held back Corpus Christi hurricane relief...Stay 43% Leave 48%

Pablo voted Stay but didn't see how that would happen...the barrage of local disputes...the disputed 2028 election...it seemed all of Texas was fixated on self-determination... Stay 44% Leave 48%

New Texas might be the first, but it wasn't the last...Pacific Northwest climate radicals would be next...Puerto Rico, Samoa, and Hawaii lost confidence in the federal government...there was talk that the Mormons were taking pre-emptive steps...

Puerto Rico, Samoa, and Hawaii lost confidence in the federal government.

Amidst the noise, no one had time to pay attention to the foreign action in South America...What did that have to do with New Texas?... Stay 44% Leave 53%...

(White Chip 1, Grey Pawn 1)

Information Disorder Machines

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.

IDMs present a unique possible and potential threat to national security and public safety. The broader concept of an IDM is not completely new and novel. In 2017 Matt Chessen authored a report for the Atlantic Council entitled, "The MADCOM Future: How Artificial Intelligence will Enhance Computational Propaganda, Reprogram Human Culture and Threaten Democracy...and What Can Be Done About It." Chessen describes the MADCOM future as a time when "Emerging artificial intelligence (AI) tools will provide propagandists radically enhanced capabilities to manipulate human minds. Human cognition is a complex system, and AI tools are very good at decoding complex systems. Interactions on social

media, browsing the Internet, and even grocery shopping provide thousands of data points from which technologists can build psychological profiles on nearly every citizen. When provided rich databases of information about us, machines will know our personalities, wants, needs, annoyances, and fears better than we know them ourselves. Over the next few years, MADCOMs—the integration of AI systems into machine-driven communications tools for use in computational propaganda—will gain enhanced ability to influence people, tailoring persuasive, distracting, or intimidating messaging toward individuals based on their unique personalities and backgrounds, a form of highly personalized propaganda."

It is the intersection of these coming technologies when combined with information disorder, weaponized, and adversarial narratives that the real threat of IDM is exposed.

The use of Information Disorder by adversaries to destabilize and discredit is not new either. During WWII a Nazi propaganda campaign was launched in 1934 and lasting throughout the war. Paul Joseph Goebbels, the Reich Minister of Propaganda, set up a shortwave radio system called the "weltrundfunksender," or "world broadcasting station." Goebbels referred to it as his "long-range propaganda artillery." Germany used the system to send false news of the "Communist Jewish conspiracy" around the world, mostly directed to North America. At the time mainstream newspapers often called the information out as propaganda and avoided repeating it. Both the NYT and the Chicago Daily Tribune specifically referred to this tactic as "fake news," attributing it not only to Germany but also to the Soviet Union in the early 1930s.

The novel aspect of IDMs are the scope and scale that emerging technologies will afford adversities and organizations. They will be able to target organizations, geographies, and groups, and then let the IDM adapt to each individual in these groups in real-time, adjusting to their changing habits, opinions, and actions. This "microtargeting," or the idea of influencing the individual to achieve macro effects, will be able to be deployed at a scale that has yet to be seen.

Adversary: A Failure of Vocabulary

adversary (n. and adj.)

ad•ver•sary

noun.

a. Law. An opposing party in a dispute or legal action.

b. gen. A person who (or occasionally a thing which) takes up an antagonistic position, or acts in a hostile manner; an antagonist, enemy, foe; (in weakened use) an opponent in a game, contest, etc.

adjective.

a. Opposing, antagonistic, hostile, inimical; adverse.

The collective threat futures identified a wide range up traditional adversaries such as foreign adversaries (FA), proxies for FA (businesses, organizations), criminals, and domestic extremists. However, the threat futures also identified organizations who would not be considered adversaries but who could use IDMs in the future to influence individuals. These non-traditional adversaries included corporations, political parties, and special interest groups.

The scope of these organizations' influence occasionally existed in illegal or prohibited areas, but often, these organizations operated in gray areas or areas that were completely legal. However, ultimately, in each threat future where these organizations were using IDMs, they caused harm to the individuals and sometimes to larger organizations, states, regions, or the entire United States.

The same techniques, as well as the same potential goals and targets, are equally apt to be used by entities traditionally considered "adversaries" by defense thinkers, as well as entities traditionally considered outside the defense purview altogether such as businesses. Any defenses against IDMs will necessarily have equal effects on businesses, organizations, domestic extremists, hostile foreign states, and so forth.

Therefore we find ourselves lacking the vocabulary to describe all of the organizations that might use IDMs. It exposes how influence in gray areas outside current law could change how we would define harm in the coming future and the nature of the response allowed by the U.S. Constitution.

The Worst of Ourselves

September 2028. Atlanta, GA

"Where are the police?" Dr. Connie Dunne thought to herself. Outside, the car protesters amassed in front of her woman's health clinic. Both sides screamed at the other...the air was electric with violence...

They were all there for her...pro, and anti... the video of her performing a careless and unsanitary late-term abortion went viral...it was fake, but that didn't seem to matter now... Connie looked at the screen in her car...

"That's where the police are..." she shook her head. Across Atlanta groups clashed... abortion, guns, immigration, race...it felt like next month's election would decide the fate of the nation. The police couldn't keep up... it was rumored they were about to declare martial law...the aggression in Europe barely registered...

Both sides screamed at the other...the air was electric with violence.

Connie's phone rang. "Hello."

"Connie, they have everything...they have everything!" Her mother was panicked and in tears.

"Wait, mom what? What do you mean? Who?"

"Someone got in...I don't know how...it's all out there...your bank account and taxes...Dad's medical records...Billy's DUI... all of it...all of it. It's all over the internet...those people..."

"Mom wait slow down..."

A savage crash and crackle of glass threw Connie back in her seat. A protester stood outside her car...crowbar in hand...

"She's over here!" he yelled to the mass. "That killer is over here!"

The protesters rushed her car.

"Mom...call, 911." Connie was sure they were going to kill her.

(Orange Pawn 2)

A Family Affair

2029. Ottumwa, IA.

They destroyed her life...took everything...her husband George...the farm...now they were after her son Tom. Lilly Smythe never knew it was happening...that it was linked...until it was almost too late...now she knew she had to fight back...

Just a year ago Lilly thought her recent rise and online fame would be good for the family farm...everyone was interested in their soybean farming technique and data analysis...but it made her a target... SCO Holdings wanted her land, the farm's intellectual property, and her silence...none of the locals knew about the foreign state behind the massive corporation...

First, they went after George...targeted him... manipulated his digital feeds...changed him... connected him with Carol...When George stole their algorithms, the farm was lost...the divorce would be final in three weeks.

When George stole their algorithms, the farm was lost.

Then they went after her... using George's betrayal...her success online...the failure of the farm...video by video... post by post...the community turned against her...the local church shunned her...

Now they went after Tom... at 13 he was impressionable... obsessed with online gaming...they used it as a way to introduce him to porn...connect him with the wrong people...Tom was withdrawing...disconnecting from his previous life...

Worried, Tom's local friends start a digital militia...reach out to Lilly...making the connection back to SCO...Lilly sees her chance...she might not be able to save her marriage or the farm, but at least she can try to save her son...

(Green Pawn 1 & 2)

The Worst of Ourselves Ourselves Against Ourselves

Multiple threat futures explored scenarios where an IDM enabled harm to come to individuals with no adversary at all. The very existence of IDM and their ability to use the worst of ourselves against ourselves, exploit confirmation biases and filter bubbles that then ultimately turn us against ourselves. Several threat futures explored the weakening of our education system, crumbling of our society, and the peaceful dissolution of the United States of America simply because of environmental pressures without a specified adversary.

In every threat future generated in the workshop, IDMs utilize individuals' fears, prejudices, beliefs, and opinions to micro-target messages, media information, and narratives. These narratives are new and uniquely personalized to influence, manipulate, and harm. IDMs use the worst parts of ourselves against us with no opinion or judgment on the individual's beliefs. The goal of the IDM is to use those beliefs to get the person to change, destabilize their values, and take actions that they normally would not.

Recent early examples of this type of activity can be seen in the 2018 paper, "Acting the Part: Examining Information Operations Within #BlackLivesMatter Discourse." The researchers studied how Twitter accounts from the Russian Internet Research Agency (RU-IRA) shaped the online discourse during the #BlackLivesMatter movement and shootings in the U.S. during 2016.

The researchers noted, "Russian information operations were active in the #BlackLivesMatter discourse (using) a network graph of retweets to learn that at least 29 of these accounts did have a meaningful presence within the information flows of this discourse... different RU-IRA accounts were participating on both "sides" of the conversation—within two structurally distinct communities."

They found that the influence activity was split nearly 50/50 between those who were pro and those where were anti, meaning the IDM was used just to fuel a negative discourse without picking aside. Although the RU-IRA's agenda in #BlackLivesMatter is not known for certain, it is clear that causing civil turmoil within the United States would only help Russian strategic goals.

Perhaps the RU-IRA are taking a page from Ender's Game in which we find the same type of narrative manipulation happening behind the scenes for selfish reasons. The siblings of the protagonist, Ender Wiggins, used the pseudonyms Locke and Demosthenes to "take sides" in an online political debate about a war that would ensue following the end of the Formic Wars against the book's alien invaders. The debate eventually led to real war on Earth (notably between the United States and the countries of the so-called Second Warsaw Pact) and Peter Wiggins, the man behind "Locke," was eventually elected Hegemon.

Business Proxies

Unique to many of the threat futures developed in the workshop were instances of state and non-state adversaries using local, national, or international corporations that acted as a front or proxy for a foreign adversary. These business proxies then would use IDMs to exert influence or even destabilize other businesses, individuals, the economy, and national security. These proxies gave distance and plausible deniability to the adversaries.

Weaponizing Authenticity

In the face of a future where foreign adversaries and organizations increasingly deploy IDMs, how might we defend against a future where the truth no longer equals the truth? If IDMs can destabilize governments and organizations, incite violence and mistrust, stoke tribalism and partisanship, then how do we counter these effects?

Two of the threat futures identified two possible counters to IDMs and explored the weaponization of truth and authenticity. Essentially they tapped into a culture that was unaware of IDMs and had grown weary and suspicious of being manipulated. In such a future, authenticity and truth can be weaponized to push back against IDM.

Catastrophes as Amplifiers

Multiple threat futures identified social, economic, or natural disaster situation that opened up a window of opportunity for an adversary or organization to deploy IDMs for political or personal gain. These catastrophes made people more vulnerable to the effect of IDMs and created a landscape where populations could be more easily destabilized. The catastrophe was a condition that allowed the effects of the IDMs to be amplified.

The Authenticity Revolution

2029.

"All human beings have three lives: public, private, and secret."
– Gabriel García Márquez,

Zhang didn't mean to become a symbol…she didn't plan to launch a revolution…she just wanted some [space] for her secret life. Zhang just cut off her data for the weekend…

She didn't realize that going offline set off a red alert in the regime…triggered her team, handlers, and representatives to contact her… an official hand delivers a letter urgently, and she is summoned to meet with the Minister…

Zhang realizes the significance of her actions… in a synthetic world, receiving something material from someone physically appearing on her doorstep signals just how far out of line she's gone. Her accounts are frozen, and her publishing keys have been removed. She has no ability to post or contact with people…

Zhang began to see the litany of the fakes that she and everyone else had come to quietly abhor…fake reports on natural disasters…fake government reports about

official corruption...fake government reports about disease...fake government reports about prosperity...fake government reports about crackdown on Muslims...fake veil of safety and security...fake reports about potential adversaries...fake government reports about the success of colonialism...fake impression that people are happy...fake genes are being added to their children...Authenticity Revolution is born...

Young people made the quiet action of taking the stairs instead of the elevator...people decide to take the scenic route to work instead of the most efficient path... people choose not to wear biometric sensors. A fashion movement blooms around anti-surveillance apparel with high design mini Faraday cage purses and messenger bags. Art is handwritten. Music is listened to live. Skateboard culture explodes.

Human beings become the malware in the system. The Revolution has begun...

Human beings become the malware in the system...AI, and data-centric bondage mechanisms become unmoored...the Revolution has begun...

(White Pawn 1&2)

NOTE: For further discussion and analysis of this scenario see appendix

Implications and Actions

"Disorder can be socially, and often personally or positionally, subjective. One person or group's 'order' is another person or group's 'disorder'. These differences of opinion can drive politics and social action. ...The more complicated the system and its social ordering, ... the more likely it is that the system will fall into a state that can be labeled disordered by some group, requiring recurring forms of remedial action to maintain the ideal order...the cost in work and resources of maintaining complex societies in their order is unrelenting. Eventually, the costs are likely to exceed the returns. ... Disorder will always appear and always has politics."

A thematic analysis of the unedited future scenarios developed by the workshop teams shows several implications. The first is that information and communication technology development leads the charge in disruptive social, political, ideological, and institutional change. Each future scenario included some form of communication means, usually, but not always, on a social media platform where content and information can be conveyed on a one-to-many basis. The future scenarios included technology not yet perfected, such as ubiquitous autonomous social credit scores influencing which "tribe" someone belongs to or real-time deep fake manipulation during a live stream event.

The second major implication is that IDMs are used to manipulate the social levers that motivate people and organizations to action. While technology changes were embedded in every scenario, it is not the case; however, that technology will determine the future; in every future prototype,

technology is a catalyst that exacerbates underlying and pre-existing social conditions. Scenarios also did not focus on traditional benchmarks of success, such as business profits or educational achievement, as a motivating force for social change; what they did focus on were the powerful forces like individuals' perception of long-standing institutions, trust in government processes, and social inequalities.

Adversaries that manipulated perception, trust or enflamed visibility of social inequalities were far more likely to incite radical social change. And not all change needs to be violent or counter-cultural; some scenarios suggested IDMs would motivate people towards change through lawful democratic processes, such as a constitutional secession of Texas.

The third significant implication is that any solution to IDM activity cannot be successful through government intervention alone. Industries that use IDM tools (e.g., AI, machine learning, targeted advertising) and those that develop the technology behind IDM tools (e.g., academia, major technology companies) have equal skin in the game and are co-responsible for the well-being of social stability.

Flags: External Indicators

The Threatcasting process not only maps possible and potential threats 10 years in the future but also attempts to identify the flags or external indicators that could happen that would suggest a specific threat future was underway. Often, flags are sequential, with less apparent precursors already in effect, and the more alarming flags still over the horizon, yet it remains unsolved how to monitor them at scope and scale.

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

TECHNOLOGY

- IDM Enabling Technology Development
  - The ability for AI and ML to specifically target an individual, processing their digital and data footprint (e.g., social media, media consumption, purchasing history, calendar, physical movement, domestic and civic activity) to specifically tailor media, messaging and data to influence their activity. Additionally, this IDM can adapt as the individual data footprint changes and morphs.
  - Advertising and marketing technologies that track individual consumer behavior and provide them personalized advertising from a preset collection of ads and messaging. This is followed by technology that can generate personal advertising in real-time.
- Opaque Technologies
  - The continued use and rise of social media applications and closed platforms that can be co-opted by adversaries and/or that are immune to government oversight and control.
  - The continued use and rise of opaque algorithms that are not auditable or accountable for their decisions.

CULTURAL & SOCIAL

- Diminishing Faith in the Union
  - Popularity of the idea of a "Constitutional crises" and increasing conflict between local and national law enforcement
  - Public perception that sentiment towards the federal government is trending negatively followed by a growing fear that the government is no longer in control and needs to be bypassed to achieve social aims.
- Truth no longer equals the Truth
  - Lack of recognized and trusted individuals and organizations that can distinguish between real and fake information, cognitive psychology, behavioral economics, and post-modern media.
  - Cultural acceptance of deep fakes as the norm leads to the ubiquity of false information.

- Public trust in traditional knowledge development deteriorates and then fails.

- Local Conflicts
  - Local and national media facilitating local echo chambers to be exploited by a bad actor.
  - Insular groups are incentivizing certain behaviors over others.
  - Continued rise of racial tensions in states and schools.
  - Increased occurrences of community-level conflicts.

- Educational Shifts
  - Lack of college matriculation and increased drop-outs.
  - Rise of private alternative degrees.
  - Companies no longer valuing college degrees.

ECONOMIC

- An economic crisis that weakens the US pushing companies to be open to unregulated Chinese investment.
- Chinese dominance in AI and tech advancements, especially those that require vast amounts of personal data to fine-tune.

CATASTROPHIC EVENTS

Catastrophes are inevitable; as a flag, they are an external indicator of increased stress and an open window for IDM exploitation and activity.

- Pandemic disease outbreak.
- Natural environmental disasters (e.g., fire, flood, famine, rising sea levels).

ADVERSARY BEHAVIOUR

- New Alliances
  - Adversary working directly with alt-right and -left, therefore, delegitimizing national conflict resolution.
  - Non-allied foreign governmental partnerships influence social media platform policies.
  - Unregulated foreign entity on social media.

- New Targets
  - Personalized adversarial (e.g., government, corporation) targeting directed at individuals and family members in different ways.

- Economic Enablers
  - Foreign governments unregulated purchasing of American companies
  - Acquisition of proprietary, personal, and other sensitive information through covert means.

Actions

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. Three high-level actions are centered on further research, technological and process tools, and regulation and oversight. These actions constitute a "whole of society" approach to problem-solving and have been applied to specific domain areas with detailed steps that can be taken.

All of these actions must be fluid to keep up with technology as it continues to change. As soon as a stopgap or detection protocol is created, adversaries will work on the way to defeat it, so there must be a dedication to continued monitoring and analysis. These action points also assume that the threat of IDMs are not because of the incremental changes that they bring about, but because they are aimed at fundamental institutional values and the future of the United States of America.

GENERAL

- Business, governmental and public recognition that IDMs are a threat to economic stability and national security
  - Conduct digital resilience campaigns.
- Cultural conversation about IDMs exploitation of the worst of ourselves against ourselves
- Develop info, facts and narrative concerning common benefits of domestic and international leadership
  - Explore new ways to deal with conflict resolution, such as making discourse and disagreement acceptable.
  - Weaponize authenticity - Use truth and authenticity as an antidote or counter to IDMs and as a pillar of democracy.
  - Recognize digital addiction as a valid health emergency.

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

- Develop general education on the limits of technology and the ability to detect deep fakes.
- Support of watchdog organizations to detect IDM activity and the conditions under which they will thrive
  - Actively work to discredit extremist information activities

MILITARY / GOVERNMENT

- Develop and deploy counter-narratives and emphasize communal global fact-checking.
- Develop laws around medical misinformation.
- Develop government standards and industry (self) policing for technology development.
- Acceptance of a valid third party in the U.S. government.
- Review of foreign purchases of US companies for awareness of proxy activity.
- Mandate tools to identify manipulative actions in AI and tech.
- Congressional commission on data, info sec, online manipulation, parents education.

- Adopt safe AI standards nationally and in collaboration with industry.
- Mandatory military draft allowing first-hand experiences to speak to the mission and trust of the military.
- Seek financial security of public schools.
- Increased awareness and action from citizens and government against misinformation sources.
- Foster organizational and local government resilience, rapid response team to expose deep fakes and misinformation during catastrophes.

ACADEMIA / EDUCATION

- Develop general education on the limits and ability to detect deep fakes.
- Develop education on stepping back from technology.
- Develop technology to backtrack all social media friends (non-AI).
- Education for the public about the consumption of networked information, legislation, and technology to regulate.
- Offer financial incentives, lower costs, and watch enrollment in post-secondary education.

Industry / Trade Association / Non-Profit

- Cooperate with governments on fact-checking without violating freedom of speech rights.
- Deploy counter-narratives, communal global fact-checking, laws around medical misinformation.
- Develop industry standards for pro-democracy/pro-privacy norms and principles around AI and social scoring or incentivizing systems.

CULTURAL / CITIZEN

- General awareness and hardening against psychological manipulation.
- Become informed parents and schools, peer groups, community.
- Seek education for the public about the consumption of networked information, legislation, and technology to regulate.
- Understand that the cloud is not your friend. "Never trust a computer you can't lift."

ADDITIONAL SOURCES NOT YET CITED

Maan, A. (2015, December 3). "Narratives are about 'meaning,' not 'truth.'" Foreign Policy. Retrieved from https://foreignpolicy.com/2015/12/03/narratives-are-about-meaning-not-truth/.

Appendix Table of Contents

Appendices

44 Appendix 1: Threatcasting Methodology

47 Appendix 2: Research Inputs: SME Transcriptions

52 Appendix 3: Research Synthesis Workbooks

54 Appendix 4: Research Synthesis Workbooks

78 Appendix 5: Futures Workbook Day One

116 Futures Workbook Day Two

160 Appendix 6: Post Analysis

Appendix 1

THREATCASTING METHODOLOGY

While the threatcasting methodology was briefly discussed at the beginning of this report, this appendix provides more details to inform "how the sausage is made".

The key to the process is the people. Participants come with a range of experiences, expertise, education, and passion. They are pre-assigned into 3-4 person groups for the duration of the process. They groups are specifically curated to take advantage of the diversity within the larger group. This small group assures that every member can express her/himself. Also the small group size allows for in-depth discussion and debate.

A fundamental component of the threatcasting process is selecting the appropriate research inputs to feed the future modeling. These focus themes are selected to explore how their evolution from today contributes to the future but also how the intersection of the focus areas' growth modify each other. To select these themes, senior leaders inside the problem space and thought leaders outside the problem space are consulted on what "keeps them up at night" or what they feel no one is focused on yet to determine the severity and urgency of the proposed themes.

Next we curate and find SMEs to inform and bring these focus areas to life within the threatcasting sessions. These SMEs are individuals that can quickly describe the current state of their domain and how it might evolve over the next decade. They provide clarity to help participants hone and define threats in the future. Transcripts for the SMEs' input are transcribed in Appendix 2.

THREATCASTING IS A FOUR PHASE METHODOLOGY.

Phase One: Research Synthesis

Research synthesis is the first phase of the threatcasting methodology. The purpose of this phase is to allow each small group to process the implications of the SME provided data while gathering the intelligence, expertise, and knowledge of the participants in the Research Synthesis Workbooks. These workbooks are located in Appendix 3.

During this phase, all participants listen to each SME's presentation but they are assigned a specific presentation on which to take notes. At the conclusion of the presentations, they break into their assigned small group. Within these groups, they identify key elements and interesting points from their assigned presentation and conduct initial analysis. They explore,

for each of these points: 1) what the larger implication of that point would be within the future, 2) characterize this as either positive or negative, and 3) list ideas for what we should do about it. The "we" is purposely broad as the input can be personal to the small group, the collected team in the room, the entire company, or the entire human race.

The output of the research analysis phase is a numbered list of these key points from the SMEs as determined by participants.

Phase Two: Futurecasting

The core of the threatcasting methodology begins with phase two of the process. Each future is based upon the Research Synthesis Workbooks.

At the start of this phase, the participants return to their small groups and select a single data point from each of the SME presentations as described in the Research Synthesis Workbook roll-up. Groups make selections via random sampling with replacement for each SME. The instrument for sampling are 20-sided dice. Without this randomness, people often pick "easy" data points that fit with their view of the future. These points establish the framework of the future environment that they will model.

After establishing the visualization of the environment, the group imagines a specific person living in that future. The group envisions who the character is, whom their family is, and the broader community with which they identify. Then the group explores where the character lives, thinks about their occupation and visualizes what constitutes their normal way of life.

The physical or digital instantiation of the problem caused by the threat is the "event". To better model and understand the event, the small group is asked a series of questions which are recorded in the worksheets in Appendix 3. Going beyond just the "5Ws" of traditional information gathering (who, what, when where, why) these prompts are specifically designed to create a more well-rounded narrative describing the threat.

Then our perspective changes and the groups see the event from the adversary's perspective; exploring potential roadblocks or barriers and thinking about new business models and practices to enable the event. We imagine the technology that would help facilitate the threat and what support systems are required. Finally, we think about the training necessary to enable this threat. This change in perspective helps the small group to better define the threat, visualize the adversary's motivations, and understand their desired end state that will be disrupted, mitigated and recovered from.

The end state of the futurecasting phase is that each small group has created a story about the future.

Phase Three: Backcasting

The third phase of threatcasting is the backcasting process. Here, still in these small groups, focused on the narrative they have created and the threat that they described – the groups think about what could be done to disrupt, mitigate, and/or recover from their defined threat actor.

During backcasting, there are two types of events that the groups explore. The first are gates. Gates are things that defenders (government, military, industry, etc) have control over that could disrupt, mitigate, and/or recover from the threat. These are things that will occur along the path from today to T+10 years. The second event type are flags. Flags are things the defenders don't have control over but once they occur, there is no going back. These flags should have a significant effect on the envisioned future. These are events we should be watching out for as heralds of the future to come.

Once the events are imagined, the small groups then timeline the actions to disrupt, mitigate, or recover from the threat. Thinking about the actionable objectives that need to occur in the next four years and also in the four years after that in order to protect against the future described threat. This iterative exercise gives the participants a chance to see how actions today can be built upon, achieving and interim goal and eventually guarding against the threat.

At the end of phase three, each small group reports out, telling the larger group a story about their person in a place with a problem. They describe the threat and what could be done to disrupt, mitigate and recover from that threat. Finally, the session ends with a discussion of the process and the collection of threats. The assembled group looks for patterns in the aggregated futures and also looks for areas that were not discussed. The session is concluded, leaving the entire group to continue to think about the futures.

Phase Four: Analysis and Final Report

Following the threatcasting session, the moderators use the Research Synthesis Workbooks as well as the small group Threatcasting Workbooks as raw data for a post-analysis. Reviewing each workbook, the team of moderators look for patterns in the futures and for areas that were not explored.

This synthesis exercise generates an aggregation of multiple futures and threats. Secondary research as well as the backcasting details from the practitioners give the team the raw data needed to make specific recommendations for near and long terms actions to be taken. The final report collects the SME inputs, the participant worksheets and the team's post analysis. The post-analysis consists of multiple clustering and aggregation exercises to determine the patterns in all of the futures modeled during the event. These clusters are then examined in light of the SME presentations, looking for possible inconsistencies or areas that need more clarification. Additionally the team highlights areas that perhaps the groups did not model but were strong themes in the SME presentations. Combining all of these together, the team makes specific recommendations for next steps and areas of action, informed by the backcasting (gates, flags, milestones) provided by the participants.

Appendix 2

RESEARCH INPUTS: SME TRANSCRIPTIONS

Three curated inputs from cross-industry experts helped inform the futures we modeled.

Transcripts of the videos are located below. The following research inputs were transcribed by machine and were not further edited. Some context might be missing or misplaced.

Benjamin T Decker

CEO of Memetica, a digital investigations consultancy

SME Video Transcript

My name is Benjamin T. Decker. I'm the founder and CEO of Medica, a digital investigations consultancy as well as a threat analyst at the global disinformation index and a contributor to the New York times visual investigations team. As any major headline will tell you, we're living in an era of weaponize paranoia, a war over the truth, and the erosion of the scientific method. In dissecting the problem at large, which we will call information disorder, we can identify three basic kinds of problematic information. Misinformation is the unintentional sharing of inaccurate information. While this information, our main bucket is the deliberate fabrication or manipulation of media mal information otherwise known as leaks are the intentional publication of private information with malintent disinformation is platform agnostic. It jumps from one site to another, often bursting from the darkest corners of the internet to the most open public squares too quickly for any one company to intervene, a meme that's down ranked on Facebook for say a false headline can still find its way to Twitter, Instagram, YouTube, or Reddit.

Malicious actors who have exploited and leveraged vulnerabilities and platform architectures to launch disinformation campaigns, online harassment and other forms of information disorder campaigns are often coordinated and anonymized forums and other fringe digital platforms for it being amplified across Facebook to exploit platform algorithms and maximize public interfacing

exposure. Memes are one of the most problematic types of content featured in any dissent formation campaign. Richard Dawkins first coined the term in 1976 defining it as a unit of cultural information spread by invitation. While Lemoore Schiffman recently updated the term by defining memes as a new form of civic participation. Mimetic just information is particularly concerning conspiracy theorists and radicalized racist who remained at the fringes for decades hijack the digital ecosystem to push ideas into the mainstream, shifting the Overton window as they claim by creating weaponized media infused with nominal partisan political issues such as immigration and national security in order to cloak more toxic views on race, gender, and religion.

The amplifiers of this content are most effective as a critical juncture along the path of red pilling, I. E. the recruitment of more mainstream and critically minded individuals into such a toxic echo chambers. In order to map the disinformation landscape, we can divide the web into four types of platforms. Open networks like Facebook, Twitter, YouTube, anonymized networks like four Chan, gab, Reddit, and discord. Secure networks like signal, telegram, WhatsApp, and then there's the dark web, each bucket of platforms, so there was a different purpose in mimetic disinformation campaigns. Ostensibly there are four general utilities, content creation, strategic communication, tactical dissemination and amplification. Just information agents, whether domestic, political operatives, far-right trolls or those acting purely for the Lowe's. Operate a bit like brush fire, arsonists setting small blazes of information in places such as four Reddit and gab where it's easy to for sparks to jump over the firebreaks and go main stream.

More bad actors often stand at the ready to fan the flames. Once in me, he was in wider circulation. Many disinformation campaigns are often defined by their ability to garner media coverage using online media strategies to push for offline consequences for the intended target. This could mean pushing a narrative so far into the mainstream that it necessitates press conferences, initiates political protests, or at its worst insights mass casualty attacks against innocent civilians. We've seen the ultimate consequences of mimetic disinformation play out in Pittsburgh, Christchurch, and most recently Poway California, where radicalize the internet is, and it's took their mimetic online activities offline, resulting in the mass murder of innocent prayer worshipers in each of the three shootings, but far more so in New Zealand, in California, the perpetrators intricately planned media operations alongside mass casualty attacks to achieve two gains, kill members of a community perceived as the oppressive enemy, and inspire others to commit similar atrocities and join a leaderless and transgression movement promoting violent extremism.

Vint Cerf, PhD (Chair) and David Bray, PhD (Executive Director)

People-Centered Internet coalition SME Video Transcript

My name is David Bray. I'm Executive Director for the People-Centered Internet Coalition. And I'm here with Vint Cerf who is both the chair for the People-Centered Internet Coalition as well as an internet luminary in terms of his role, pivotal role in helping to co-create the internet. And we're here to talk to you the about the challenges of dealing with polarizing misinformation and social wedges that are created and how we collectively might play a role in as part of open societies to try and address it. And so with that, I'll start with asking you a provocative sort of thought experiment in terms of what could we do to

help people become more aware of their biases, confirmation bias when they're locked in and they're no longer receptive to facts swaying their position.

Vint Cerf:
So this is actually a real challenge because not everyone wants to be reminded that they have biases and they don't want to be told you're wrong about something or your beliefs around, uh, this, this sort of that you can't tell me I'm wrong. Attitude is pretty hard to get over. So, I think we have to be more subtle about how we help people discover their biases or their...[pauses]

David Bray:
Cognitive ease?

Vint Cerf:
Well, it's not cognitive ease. It's the problem when you get into confirmation bias, that's the problem. We get people who are, uh, get comfortable in a feedback loop that says the only thing that must be true is what they believe, et cetera. I know that there are some people who when they encounter misinformation or what they think might be misinformation, uh, will actively go and look for Snopes, for example, to see whether something is known to be, uh, simply, uh, you know, an urban legend. But not everyone's willing to do that. We should draw attention to those kinds of sources of information that are available and we want to highlight information sources that we believe are trustable. Um, but I think as you imply and all of this, we have to find, you use the term cognitive ease. I think that's very valuable. How do we make people comfortable asking questions? Like, where did this information come from?

David Bray:
Excellent. And, and add my own thoughts about this there. There may need to be efforts to try and monitor and help people be aware of in the last five or six actions that you've done. You've tended to go this way and you might be okay with it. Or the technology could actually hold a reflection to ourselves and say, here at least when it comes to either hiring biases or approaching new sources, you tend to go to these outlets. It's almost like we need to have the ability to hold a mirror up to ourselves and let us know if we, we seem to be consistently going one way and maybe we're okay with that. But in this increasingly challenging world in which there's all these different information sources, we need to embody what Lincoln said, which is I do not like this man. I must get to know him better.

Vint Cerf:
So speaking of this, in mirrors in particular, the internet in some ways is a mirror of this society thing we live in. Certainly, does social media, as an example. And if we don't like what we see in the mirror, changing the mirror doesn't help very much. Uh, even though there are people who would say, well, can I just suppress this information? Can I just filter it out so that nobody will see it? That's called censorship. And even though, uh, we generally tend away from that here in the U S and because of our freedom of speech commitment. It does raise an interesting question. At what point is, is it, uh, censorship that that's bad, uh, when you decide to suppress certain information and when is it a question of either national security or safety, um, example, you know, uh, injections, uh, of vaccinations cause autism is not true. It's been proven that to be true. And yet some people still believe it. At what point do we decide we should filter that out?

David Bray:
That is the, the, the great question that hopefully everyone gathered at Arizona state university might be able to help answer, Oh,

add my own sort of lens to that, which is we've tolerated to the degree uses of confirmation bias and cognitive easing for the purposes of whether it's advertisements or marketing where something's repeated to you over and over and now you really want to buy it. Or for political rhetoric purposes and political influence purposes where maybe something is skewed in terms of how it's shared with the public or it's repeated enough. And so, it's trying to make you think, and the interesting question is, at what point is that kind of like removing wrinkles through Botox? But the trouble is botulism toxin can also paralyze you, stop you breathing or even kill you. The question is, when are we okay with skewed information, misinformation or using cognitive ease effects for advertisements or political rhetoric? And when do we draw the line and say, okay, now we're actually beginning to kill society. And I think that's going to be the hard question and we look forward to what people can say.

Vint Cerf:
The sort of the core question is, at what point is the cure worse than the disease?

R. Bradley Snyder

President New Amsterdam Consulting
Executive Director Dion Initiative for Child Well-Being and Bullying-Prevention
Award-Winning Researcher, Author, Activist, and Aging Malcontent
SME Video Transcript

The generation of children born somewhere after the mid-1990s is alternatively known as the "Plurals Generation," the "Homeland Generation," and even "Generation Z." And it is the most diverse generation in the history of the United States. It's diverse not only in terms of its demographics, but it's diverse in terms of its friends' circles and in terms of its preferences, its likes and its dislikes. Some of this diversity stems from things that we, as the adults, have done for them. First, we've created a society that has become more equitable and has increasingly valued diversity, but we've also given them powerful, powerful digital tools that have allowed them to experience the world without borders, without constraints. They'd been called "digital natives" because the tools that they had from the earliest memories were capable of all these amazing things, and they were always with them. And, as a result, they've started to expect certain things from their experience.

First of all, they expect that, if they want to participate in a story, in a campaign, in a movement, they want to be able to do that wherever and whenever they are and, kind of, however they want to participate. It's easiest to think of in terms of a story like Harry Potter. A child who enjoys the story Harry Potter wants to be able to sometimes watch the movies when they're in that mood. Sometimes they want to be able to watch short clips about the movie. Sometimes they might want to see a video of somebody who is a lot like them talking about what they like about the movie. Sometimes they might want to read stories that were created by other people that liked the movie as much as they do that expand that original story. Sometimes they want to be able to play a video game about that story so that they can feel like they're actually inside it, and the powerful tools that we've given them as adults allow them to do that, to participate in that story wherever, whenever, and however they want to.

The downside, of course, is that if you have a story, if you have a campaign if you have a

product that doesn't allow them to experience it in all of these different ways that the current generation wants to, well they'll leave that story, that product, that campaign. They'll find a different one, or maybe they might even create their own. You know, starting in the late fifties we moved as a society from a more authoritarian way of parenting to a more participatory style. What that means is over the last seven decades, we've slowly started to involve our children in more decision-making processes, and we've exposed them to more of our own feelings and our own experiences as adults. Consequently, our kids are pretty stressed. This current generation has levels of stress that have never been seen before, and it's partially because not only do they have their own stress of trying to become fully formed humans in a very complicated world, but they also now experience the stress of the adults around them. As a result, this generation is a very serious generation. They're very, very committed to causes. They're committed to their own family's financial stability, but they're also committed to a more equitable, more ecological future for everyone, and they understand hard work and they are willing to put in the hard work to make those things a reality. It's a pretty amazing generation. I'm looking forward to seeing what they do.

Appendix 3

Further Analysis of Weaponizing Authenticity

"Weaponized Authenticity" and "The Authenticity Revolution" refer to the scenario in which deep fakes and similar ever-more-potent in-development weapons in the narrative attack arsenal become ubiquitous. As a result, increasing numbers of people no longer believe anything they view or read or hear on the internet.

This loss of trust leads to the battle cry, "Never trust a truth you can't touch." (This is an homage – conscious or not – to the Enlightenment principle that truth can be recognized only by the evidence of the human senses to which reason has been applied.)

In this scenario, The Authenticity Revolution starts behind the Chinese Great Firewall. All indicators suggest this scenario is already nascent today. As this future unfolds, and the internet fragments, other armored and ring-fenced communities emerge where there is no access to verifiable external reality via electronic means. In those places, similar home-grown revolts also spread.

These revolts are against anything perceived as possibly being controlled and exploited by others in a malicious fashion. Especially in highly controlled societies, innocent behavior becomes a signifier of those sympathizing with or participating in the revolution (e.g., taking the stairs rather than using elevator technology).

"The messages are a potent amalgam [in China] of contempt for railway authorities, suspicion of government explanations and shoe-leather journalism by citizens and professionals alike.

"From a Hubei Province blogger: "I just watched the news on the train crash in Wenzhou, but I feel like I still don't even know what happened. Nothing is reliable anymore. I feel like I can't even believe the weather forecast. Is there anything that we can still trust?"

"The government censors assigned to monitor public opinion have let most, though hardly all of the weibo posts stream onto the Web unimpeded. However, many experts say they are riding a tiger. For the very nature of Weibo posts, which spread faster than censors can react, makes weibos beyond easy control. Moreover, their mushrooming popularity makes controlling them a delicate matter."

"A worker comes to Beijing, to Communist Party headquarters, and asks to see Chairman Mao.

A soldier stops him. "You can't see Mao," he says. "He's dead."

The worker returns the next day and again asks for Mao. The same soldier turns him away: "You can't see him. He's dead."

The third day, the worker returns, and insists: "I must see Chairman Mao."

The soldier loses his temper. “I told you yesterday and the day before that. Chairman Mao is dead. Dead! Dead! Dead!”

“I know,” says the worker, with a smile. “I just love hearing you say it.”

That is the first joke I remember learning. I was 6 years old when I committed it to memory and started retelling it.

You may say that a small child telling a joke like that is “not normal.” Then again, we’re seeing and hearing a lot these days that is “not normal.” It’s what we say when we see slippage in our democracies when authoritarian leaders violate norms.”

“A seemingly youthful Chinese vlogger known as “Your Highness Qiao Biluo” was outed to be a 58-year-old woman when the face filtering software she used to make her look younger glitched during a Livestream.

“The vlogger used a beauty filter to pose as a much younger-looking woman on Chinese live streaming website Doyu. During a live stream with a different vlogger, Qiao Biluo’s face filtering software stopped working, revealing her true likeness to her viewers — and raising questions about how we present ourselves on the web.”

The revolt against the influencers:

“Over lunch this spring, Nikola Burnett, a 15-year-old who always carries two cameras — one film and one digital — sat staring at an Instagram selfie, perplexed. The subject was Miquela Sousa, better known as Lil Miquela, a 19-year-old Brazilian-American model, musical artist, and influencer with over a million Instagram followers, who is computer-generated. “She’s not real, right?” Nikola asked me shyly. She knew the answer, but something about Miquela made her question what her eyes were telling her.”

“These twenty acres feel like both a real and a symbolic bulwark between a receding life of authenticity and the digital realm of vicarious experience. “There are things about the modern world that I am not going to get on board with,” Manning says as we pause to admire a persimmon tree that figures into several of his poems.”

“Generally, millennials and Gen Z have a more nuanced understanding of advertising and manipulation than any generation before them. They see through the tricks of the trade and instead want something genuine.”

---

these could serve as examples of push back such as Instagram “influencers.”

https://www.nytimes.com/2019/04/03/world/philippines-hotel-influencers-social-media.html

https://www.theatlantic.com/technology/archive/2019/04/influencers-are-abandoning-instagram-look/587803/

possibly Twitter bots,

https://www.theverge.com/2017/8/13/16125852/identify-twitter-bot-botometer-spambot-program

https://www.nbcnews.com/tech/tech-news/after-mueller-report-twitter-bots-pushed-russiagate-hoax-narrative-n997441

even recent LinkedIn example (A spy reportedly used an AI-generated profile picture to connect with sources on LinkedIn)

https://www.theverge.com/2019/6/13/18677341/ai-generated-fake-faces-spy-linked-in-contacts-associated-press

Appendix 4

IDM RESEARCH SYNTHESIS WORKBOOKS

After listening to the three-curated inputs each group, assigned to one speaker, synthesized what they heard and plotted data points accordingly. With each data point they carefully examined implications of this data point, if the implication was positive or negative, and any thoughts around what might be done to encourage the positive data point or mitigate the negative. The first twelve pages of this appendix contain the role up of all the groups' data points for each speaker. This was necessary for the threatcasting inputs. The second half of this appendix shows all the raw data for each group individually.

The information found in the following pages is raw data and has not been spell checked or edited in any manner.

Speaker 1 Consolidated				
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Diverse: demographics, preferences, likes/dislikes	Contributes to **fragmentation across society** (but isn't the main driver of it); also: hopeful and idealistic; forcing traditional organizations (i.e. churches, universities) to relook traditions of acceptance	positive	Either increase tribalism & fragmentation OR increase inclusiveness at potentially the cost of maintaining traditions
2	Given powerful digital tools "digital natives"	Borderless world - may be providing basis for nativism and xenophobia; sexual contact starts later, but exposure to pornography is earlier and more intense —> easier to isolate self than create relationships; physical geography matters less	negative	Encourage non-geographic similarity and connection; must consider the implications of a technological fix
3	Universal acceptance	Also seeing a **rise in identity politics**	positive	Generate support from large geographically diverse groups
4	Expectations: participate whenever, wherever, however	If there are products w/o experiental expectations - leave or create own; relying on own experiences is a cognitive bias which leads to easier acceptance of tribal narrative; "Truth," "Belief," "Acceptance," and "Identity" are different	negative	Opportunity to drive people off products (or platforms) or towards products (or platforms) based on participatory expectations; opportunities to "detox" or take a break from tech
5	Marketing and product-oriented organizations control the technology	Limiting or controlling the tech is not viable; too many interests; dual-use with positive/negative uses; whole of society contexts make it useful for many different domains	negative	
6	Participatory parenting	Conservative person tends to more authoritarian parenting style —> specific to class structures and world view; more liberal person tend to more participatory parenting style; context of course matters;	negative	Cutting off from mainstream culture (i.e. home schooling) due to threat that kids are being influenced too strongly
7	High stress dealing with own youth and adult situations	High stress **relies heavily on heuristics** (i.e. one's "narrative") rather than "system 2" rational analysis; External manipulator can use this info and fear, anger, other powerful behavior drivers to move to action	negative	add delays into the system, so the cortisol responses drop
8	Committed to equity and own family finances	"Equity" is a trick word —> to libertarian, equity means keep what you earn; to others, (egalitarians) equity means sharing amongst all;	positive	
9	What is impact of older generation?	Lack of "adult" mentorship; use of "adult" organizations to **communicate to next generation** (builds "tribal" societies); victory of Rosseau over Voltaire	negative Transition to US tribalism may have future benefits akin to other tribal structures	form interest-based connections across generations
10	Perspective from privileged American gen Z	Brains develop differently ; two-tiered culture (access vs non-access)	negative	form interest-based connections across priviledge/non
11	Hard to descern misinformation and disinformation	in order to know facts you have to investigate multiple sources, and shorter attentional span and overwelming data makes a single individual might be interesting in digging for the truth. Only really care if it is entertaining, but fact based narrative is not required. Distrust of fact based scientific narrative that cannot be experienced.	Negative as very hard to show bad behavior and also hard to prove validity of soures or arguments. (The Death of Expertise) the digitialize of online sources and broad availailbity of information lets all become experts. Still takes time to ingest data. How do you acknowledge experts. Involvement of experts in false narratives discredits experts. Deligitimization of these experts.	
12	Friend cycles and preferences and invovlement in choosing	Diversity of Friends and friend groups causes the Z to discredit experts and "think tanks" and as a result will not provide the market as they walk away from the nonexperiential learning with high bar to entry.	We have brought them into the decision making process and will expect to be included. The deffernce to experts is going to be problematic.	need to have think tanks, educational institutions to have transparent funding reports to trace the funding and establish the ligitiamacy and bias of funding. Need to engage in countering misinformation to show the real value of experts. They must provide solid, scientific based arguements and aggressively discret false information. Not enought to prove the point, need to also address dirstractors or differing opinions.
13	Online Friends are Real	trust element in the internet	Skills to identify online charlatans and in person are different. However, we have to admit we have met people in real life that were trying to decieve us or market to us.	
14	Working for good and value of fairness	project fairness onto others on the internet and reject the idea that others would be trying to deceive them for naefarious reasons.	Will probably not project across cultures. VContactia and other russian media are different and discimating the false narratives aggressively for their own purposes. Campaigns have to address the impact on the social good or create the alignment with the social.	Important to be looking at across cultures and platforms to track and enforce across the russian networks. Similiar to UN need to be created to regulate Facebook, it cannot be just be ruled by US Law. A new design of thinking of companies vs countries. Beyond Westfalia.
15	Experiential Learning on and off line, and participate in the narrative	can't control how the experiences are constrained, difficult to get different opinion	Lack of normative causes them to distrust everyone, but trust themselves. The volumne of variety of narratives and truth gets disregarded.	Not enough to just put fact based information into the public square. Need to explain why they need to value a particular piece of truthfull infomration. We need to establish new metrics of trust and find ways to teach both what is right as well as incorrect
16	Their resources are online, mulitute of public squares online	They will look for diversity of opinion on the internet as a part of their explortion but it is very hard with architures of internet to break into differnt thoughts. Russian propaganda is also online but in different forums so you will not find them if you are not on those networks.	Believe that the resources reflect the entire world, but are really only a fraction.	Babel Fish type technologies to have real time translations across language barriers to facilitate a truly global perspective.
17	Enjoy reflections by friends on these they like, not on same tools as the other generations. Utube Channels and peers networks	Reinforcement of bias and huge amount of information availalbe to confirm their biases. The ability to spend huge amounts of time on one topic limits the time to absorb the breath of society and issues across society.	Positive if you can influence the peer groups, and will be equally difficult for all narratives.	Need to find ways to convince influential members of peer and get these influencers to replace the role of experts and authority.
18	Many tasks so work to complete to get to next - speed of injestion	A huge amount of stimuli can mask lack of depth	Impression bias and clickbait type informtion can cause messages to be transmitted unintentially and operating at the same speed as information is critical.	
19	Tools are always on so need to finish now	Increase of stress for tasks that cannot be finished quickly, hard to keep the huge list of priorities that need to come back to and attempt to finish. Expect to be able to participate however, whenever and whereever they desire		how do we create the scaffolding to allow the information to stick and also have the informaiton when it is requested.

20	Diversity among Z and between millentials	How do you educate and inform such a diverse population that are coming with such a diverse backgrouds as well as interests. Will walk away if not invovled, but need multiple narratives to engage across the society,	Develop of the message/narrative can take longer than the "news cycle" causing the truth to be shooting after the duck.	Method as well as the product becomes very important. If you choose and succeed with the audience, you still only have a small part. Levels of differsity and interestes are consistenty changing.
21	Children born after mid-90s are most diverse in terms of friend circles and preferences. Both societal values and because of the digital tools available	(Assumption: valuing diversity means diversity within social circles) - This suggests that there is more potential for people to be exposed to view points and experiences different from their own	Positive	1. Create a campaign that leverages this trend in Gen Z as a motivation for the older generations to do the same thing. 2. Campaign targeting Gen Z to encourage expanding beyond diverse social circles into valuing discourse
22		(Assumption: valuing diversity means that the differences between social circles is greater) - this suggests groups are getting smaller and the distance between them is increasing	Negative	1. Campaign targeting Gen Z similar to early 20th Cent to encourage activities that are social good (meeting other people, engaging in discussion) ref Heinekin ad about building a bar
23	They expect to be able to participate in all the data sources (cause, film, game, etc...) they have access to and want to be able to participate in a number of ways and situations	The communication that wins isn't just based on the message, it is also based on the medium that lets Gen Z interact in the ways they want. Which means merit of message is less important than sophistication of medium (which biases for money and resources) and less important than accessibility (the more ways you deliver the message the more likely you are to win - Baader Meinhoff phenomenon)	Negative	Come up with multi-modal methods of communication rather than old fashioned PSAs/websites. Personalization; target audiences need to be able to relate deeply.
24	They are more stressed due to their parents sharing more about what is stressing them	Gen Z is indoctrinated into high stress world views at a very early age, which makes it hard to get them to even start to think about how to question those views	Negative	This is not really new, parents always indoctrinate their children. Focus on education around critical thinking
25		The childish behavior (sharing of weaponized memes, etc...) of parents is now much more visible to children due to them being on the same social media platforms	negative	**Ad campaigns targeting parents to stop role modeling this behavior - this generation's version of "I learned it from watching you dad!"**
26		Children that grow up watching their parents spreading weaponized memes will think there's nothing wrong with having political leaders who behave that way and in fact may prefer it	negative	1. Focus on education, setting examples and role models of what good behavior looks like - (ala sex ed, stop smoking). 2. Create policy that prevents echo chambers
27	Very committed to causes, more serious, understand hard work	Everything they are commited to is utterly critical to saving the world (regardless of political leaning). They are much more likely to be tribal	negative	Create more opportunities for cross-group collaboration
28		They have the potential to do great things and to lean into things that are uncomfortable	positive	1. Create more opportunities for cross-group collaboration. 2. Use social media to amplify spaces for constructive collaboration **3. Drive the concept of self-policing; communities are responsible for holding their most extreme members to a standard of good behavior that they would want to see from the other side**
29	They value diversity and want to create more equitable society & environment	Given the opportunity they might be willing to actually voluntarily do work to make this happen	positive	Create a public service program for people to participate in creating positive environments
30	This generation has never had "no access" to the Internet			
31	This generation has had social media from the start			
32	World wide this gen pays attention to the latest communication trends and don't want to be left behind			
33	This generation has had the war on terror for their entire lives			
34	People gain their identity from their groups and we are seeing more fragmentation into smaller and smaller groups			
35	Flawed analysis that got us to the discussion of GEN Z.	The perceived power distance between GEN Z and older generation is an actual reality vs belief.	Initial reaction across the board is negative for all of these data points and implications however we have not fleshed out.	Drink a beer!
36	Protests challenging DoD working with corporate America. The generation should influence what projects their companies undertake not just what individual projects "they" undertake.	1% of the population having experience with the DoD. How does the DoD stay on the forefront of the free world when an inherant distrust is present to what the DoD does.		
37	What drives these technological companies? Generation Z has more leverage with these companies. Their work will have impact not two years from now but two weeks from now.	Is it money, is it resources or is perception that drives these companies? To what extent is their a tension of a company that its purpose is to make money vice provide greater good to the community? Global companiys (perponderance of US companies) are driven by GEN desire. Compromise maybe the true driving initiative. Company is optimizing not soley based on profit. The compromise on the bottom line vs other values.		
38	GEN Z willing to work hard but need to see immediate impact.	The need for physical communities will diminish. Perhaps the pressures to hold them together is diminishing or becoming harder	Negative	
39	Active roles in political and social activities.	Equity issues of relationships as employees of a company vise GEN Z ers as consumers of society. GEN Z will not give up things like Twitter even though it has some of the most hateful and divisiness present.		
40	Millenials and GEN Z will be 75% of the workforce... WOW!			
41	Technology is disaggregating society.	The amazon example driving companies to certain methodologies... shipping to home vs travelling out to purchase things.		
42	The Industrial Revolution made the US what it is but the US is no longer in that econmic state.	Institution are inadequate to address the present much less the future and will brake the paradigm.		
43	Any place, Anytime, Anyway			
44	Self organization takes place now in cyberspce because of the limits of the terrestrial space.			

Speaker 2 Consolidated				
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Censorship	Is this too broad of an issue?	Can be either	
2	Cognitive Ease	entice people to self-reflection, and then engage with learn, and potentially embrace new truths?	Neither	If you want to start a revolution, throw a better party.
3	Confirmation Bias	People on all sides virtual signaling, the internet as a mirror of both the society we live in an the identities we wish to fortify.		
4	how to make people care about	throw a better "party" to entice		
5	the internet as a mirror	Distorted reflection as a hall of mirrors - opportunity to amplify certain divisive features, perpetuate them, threaten/exclude other perspectives	Both	As internet become more integrated into society, internet less of a mirror because becomes and extension of individual selves - As becomes more integrated, less ability for anonymity
6	self harm/otherize	Self-destructive behavior is no longer *self* destructive in a connected word.		
7	so much of democracy is about the process of contesting knowledge. it works when we're able to have a healthy media/knowledge ecosystem. the fact that so much communication happens out side of the view of media	Ease of access to constantly-present information		
8	things are subtle:memes, not quoting sources, complexity of language, signals&signaling, rhyming as away of signaling meme, playground bullying with machine learning, signals get the confirmation bias going	Journalists, fact-checking, and knowledging contesting / synthesis breaks down. If '90 percent' of human communication is non-verbal, what's the non-verbal communication equilivant of online.		What's the immune system for toxic signaling and non-verbal communication and behaviors. What's the relationship between signals, and behaviors? You could argue the best influence attacks are based on hidden or explicit signals that get past a) algorithmic detection b) journalism oversight, c) community immune systems to disinformation
9	How to get tone in text, could you identify when someone wants to start a fight, e.g. ends with a period	People defer based on subtlties in real life (appearance, gender, height, percieved authority) - have we identified what causes people to defer authority online? Can that be utilized as the subtle way to promote self-reflection?		
10	what's the non-verbal in digital communication			
11				
12	Determining a need for censorship and regulating potentially increasingly-radical conversation/thought			Our Design Victory Condition is to render censorship unnecessary? What's the healthy, non-authoritan digital panopticion? How do we reintroduce, non-extreme, human level consequences, build famility and community connect and empathy, and deter toxic behavior. Lots of little sub-conscious corrections, you don't have to internalize and take it personally, or have it feel like an attack. De-escalation, healing, re-connection to the community are built into the correction in ADDITION to accountability. This happens at the individual level, as well as groups within a community (which probably requires a similar, but different kind of reconciliation, negotiation)
13	Tunnel vision, desperation in the face of change	need to protect homeland, need to sustain self (economically, socially), respond to state-based/non-state-based narrative attacks		principles-based approach to information warfare; defending definite truths - promoting democracy vs defending democracy and deciding on whether to adopt multilateralism
14	Lack of transparency	People have the right to know who's whispering in their ear		policy, police the hell out of the platforms to be transparent
15	media and platforms as business	Business model of maximising clicks and ad revenue drives content that is not necessarily journalistic of balanced		regulation of platforms or education of consumers?
16	censorship	Balance of freedom of speech and control		regulate platforms and culture of conversation, not content; self-regulation of communities (platforms that give more ability to self-police, assert rules)
17	critical thinking, education	critical thinkers, media literate audience knows to ask "why"? perpetual learning; constantly reinventing the quality of public discussion		education (discussion, debate); open discussion space and culture; role of good old investigative journalism, the least profitable part of the medi business;
18	peoples preconcieved notions, tribalism, identity politics	A lot of public communications is based on stereotypes and in-groupism		
19	targeting the enemy with tools we cannot target our own people with			
20	Information segregation, information bubbles	Creates echo chambers; feeds confirmation bias	Negative	
21	extremist content (ISIS, etc.)	Insighting violence in the public sphere	Negative	transparency, notice and takedown
22	attention economy	attractive content is on the shallow end		stop payng attention to the extremists; educating an audience to be demanding
23	Didnt make correlation between narrative and confirmation bias	not clear how cognitive bias plays out	both	identify how confiermation bias promotes esisting narrtives; elaborate additional cognitive biases that might impact narrtive acceptance
24	which narratives more likely to be effective	resource allocation; amelioration strategies		examine the role of emotion; examime the role of communities/bubbles

25	can't change the mirror	have to offer replacement if taking about previous narrative; cognitive ease = must make alternative as easy to digest more desirable explanation for the world	negative	re-tool messaging away from "you are wrong" to "here is why the alternative benefits you"; also, make that replacement message easy to disest.
25	botox is a limited treatment	correction has a role	both	better understand which messages are most dangerous (and craft direct counters); identify which narratives are better innoculated with alternative narratives
27	Potential for the cure to be worse than the disease	Dealing with misinformation may be better than changing a foundational American value (1st Amendment/Freedom of Speech/Access to Information	negative	Compare the risks of allowing misinformation campaigns to continue with the consequences of limiting speech/access to information; monitor the impact of private actors limiting speech and/or preventing access to platforms (Alex Jones, InfoWars etc.);
28	what if I dont want to look in a mirror	many people feel disinformation a problem, but most won't correct their biases; most people think that misinformatiion is problem for *other* people	negative	educate the next generation on good information hygeine;
29	I do not like the man. I need to get to know him better	Bubbles are a major part of the current problem -- a broader community of sources helps protect against biases	positive	Encourage news consumers to draw from a borader range of sources; promote mediated/curated discussion across online communities
30	trust is super important	people are more likely to believe a friend than a news reporter	both	news institutions need to rebuild trust; amelioration strategies must leverage grass-roots energy
31	which narratives more likely to be counteracted	resource allocation; amelioration strategies		examine the role of emotion; examime the role of communities/bubbles
32	social wedge	We want people to leave bubbles of social media, however is higher education becoming a problem? Controversial thinkers being pushed out of institutions as they are making students uncomfortable. We are training minds early on to opperate in bubble	negative	institutional awareness of differing intellectual thought as aide to stufent minds. Socratic method
33	Who is the arbiter of veracity?	Democratic action requires an informed citizenry, so accurate information is a public good, but at the same time free speech is a cherished, national-identity-forming value, which puts into tension establishing an entity for vetting information accuracy vs. stifling free speech	positive and negative	Provide some easily digestible information provenance to help people verify information. People have to care that they are being gamed, before they can begin to fight the problem. Some people are blissfully ignorant; some people have bigger problems than to care about the existential threat of misinformation. People think "the media" are at fault. Truth is socially constructed, so it is not unconditional. Where is the common value?
34	socio-economic drivers of generational perspective (what's important) and values	today's Gen Z'ers and Millenials have a different economic outlook and that drives new values (sharing economy vs. private property ownership) and potentially drive perspectives on the value of socio-political institutions (education, press, govt) as beneficial	risk, with potential negatives; society in change is susceptible to mis/disinformation, disruption	need resilient institutions and adaptive to societal change that acknowledges how people operate in today's world and what they care about.
35	privacy is changing	used to be that there was a specific difference between private informatioin and public information; public spaces and private spaces; separation between public/work, public and social, private and social, private/family, etc; --now those borders have eroded both by virtue of the intrusion of media/social media, and by reconceptualizations (and exploitations) of what is personal/private/public	comes with risk	we need greater awareness of the changing nature of privacy; how do you develop empathy online with only screen-based cues?
36	off shoring of critical infrastructure--pharmaceutical, manufacture	foreign adversaries it can be used for social credit or other means of exploiting citizens; can disrupt institutions and exploit fear.	comes with risk	secure supply chain with blockchain or other tools
37	off shoring of critical infrastructure--technology talent	foreign adversaries it can be used for social credit or other means of exploiting citizens; can disrupt institutions and exploit fear.	comes with risk	
38	increasingly complicated nature of (nearly every) aspect of society from health care to economy, etc.	rise of populism: sweeping, simplified, emotional arguments to bucket a range of complicated problems into a simplied 'solution' that is really simply a route to power consolidation by the perpetrator of the simplification	comes with risk	
39	education			

Speaker 3 Consolidated				
#	Data Point	Implication	Positive or Negative?	What should we do?
1	"Weaponized paranoia" is a real threat	People are getting more aware, but it's also Increasingly sophisticated on the practce	Positive - people more aware that this is an issue. Negative - bad actors are getting increasingly sophisticated. Where is real education coming around this? Possibly may erode science and democratic institutions	Use tools, people, technology to identify early - what is misinformation? Leverage technology to identify it. Need education, critical thinking throughout population
2	Using information deliberately to influence: misinformation, disinformation, malinformation	How do you identify right information vs. disinformation	Positive: more attention in figuring Negative: Need more trained workers to find and stop bad behavior is toxic. Rise in mental health challenges.	
3	New ways to sift through analysis of information (AI programs, more off the shelf options)	Who designs the programs that sift the information? How do we know it's accurate? How do you make the algorhims fair and open (FAIR ML)	Negative: How do we determine what is "fair"?	
4	Track disinformation campaigns to study and categorize the type of disinformation campaigns			
5	Information wars on 2+3 main threats: China & Russia; North Korea, Iran, violent extremism	Move from weapon systems in tradition sense, to information systems. Who is leading that? What is the strategy?		
6	Platform agnostic - many types of platforms and media that it can go through	Quick and dynamic. Can spread from anywhere and to anywhere		
7	Integrated attacks - information designed to trigger action designed to get more media and recruit more actors	It can be sourced and scaled from anywhere	Harder to identify what's real and what should require qction. What do you pick to counter?	
8	Immediate amplication through toxic ecochambers (use to amplify disinformation)	More you let it go, the dangerous it becomes	How do you balance regulation with free speech?	More regulation (self regulation or govt) to identify and take extreme views off the platform. Investigate business models around extreme behavior
9	Traditional warfair being applied to infomration: Techniques, Tactics & Procedures		Do all countries regulate by the same values?	
10	Cyber-forensics used to discover bad actors on the web to discover coordinated attacks	Need to find people who can create programs to stay abreast of tactics and local cultural context (language is key!)	Negative: where will the talent come from?	
11	Meme-factories generating disinformation	What makes memes go is how well it gets absorbed. How it gets adapted. In closed societies, they are using symbols to get around censorship (rice + bunny rabbit for #metoo)		
12	More disinformation campaigns impacting more sectors (elections, corporation reputations, etc.)		Who is the watch dog?	New standards need to get created? Who is the watch dog
13	Rise of deep fakes			
14	Increased investment - public and private funding to fuel and combat the issue			
15	malinformation is true, disinformation is false			
16	meme is something that spreads like a disease vector; what's new is memes that cause action in the real world.	memes do not require literacty -- can be consumed as cat videos		
17	dependent on receptive audiences			
18	digital landscape/terrain			
19	amplification/manipulation			
20	testing at scale/speed/rapid feedback loops			
21	influence/interference			
22	"platforms" content/atomic unit			
23	diffusion			
24	adversarial behavior intent	divide/polarize		
25	what happened when people decided that gay marriage was okay?			
26	everything you thought you knew was wrong events	speed that these events happens		
27	what happened when people decided marijuan was okay?			
28	2nd and 3rd degree implications of current influence operations			
29	75% of the workforce is going to be gen z and millenial			
30	impact of deep fakes?			
31	can the chaos creators open to attack by their own people?			
32	can the muslims attack the chinese regime?			
33	Assume the tools to create all forms of media effectively have become ubiquitous: ai, augmented reality, deep fake videos, games, movies, media platforms, social networks.			
34	Audience Receptivity: Gen Z example of having media everywhere in multiple forms? And how that effects our values and ethics? Synthetic vs. Natural, Transcending our digital space,	A new set of values, a cultural revolution to a spiritual revolution, against the tyrannies that seeme inevitable --suppose there is a reaction to all the things that are scaring the shit out of us to one that is focused on ethics and values...people are looking for bedrock. A spiritual revolution. A mass movement towards real.		
35	ethics? values?			
36	What is the path to everything you thought you knew was wrong event?			
37	What are the TTP's to piss on things we know now that are wrong?			
38	Post-Truth Society	Tribal truths rule		
39	Online social media platforms	Easy to connect and amplify, weaponize		
40	Conspiracy theories	Persistent alternative interpretations of reality and who is in control, narrative trumps truth		
41	Faux insiders	Creation of a false credibility base, appealing to emotions		

42	Alt identities	Bots, fake IDs, malicious actors		
43	Troll farms	Industrialized astroturfing and grassroots propaganda		
44	Propaganda for all	Anyone can propangadize, does not require state-level resources		
45	Cross-border interest groups	Digital tech allows interest groups to act globally		
46	Radical levelling	End of expertise, anyone can speak out, democratized voice and participation		
47	Editable history	Blur truths, revisionism		
48	Accelerationsim	Speed up events		
49	Millenialism / Apocalyptics			
50	Social Fragmentation	self-imposed segregration?		
51	Hybrid State Warfare			
52	Ideology over epistemology			
53	Globalization favors closed societies	Open societes are vulnerable to state-sponsored bad actors		
54	audio/video/Photo manipulation	Easy to manage perceptions or edit reality		
55	Revolution rhetoric			
56	Chaos is a ladder	Fomenting chaos creates opportunities for excluded populations		
57	Crisis Opportunism			
58	Who is the threat actor?			
59	Funded, coopted media	narratives reinforced / transferred into the mainstream / enhanced credibility		
60	Technology ignorance	Tech savvy people can manipulate the ignorant		
61	Gambler doubling down/sunk cost falacies			
62	Long term effects of weaponized narrative (algorhithm based childrens videos)			
63	2020 is going to be a mess			
64	Narrative Trumps Reality	the end of expertise, a society needs a shared narrative to exist	Both	
65	People are hungry for authority	Absence of credible authority (idols) creates opportunities for multiple sources of truth	Negative	
66	Information/disinformation is platform agnostic	Easily accessible anywhere; information/disinformation can jump platforms; solutions often platfom specific;	Positive - lots of channels, lots of diversity, lots of options; Negative- disinformation is very hard to combat; no single solution	Platforms should do risk modeling and collaborate on solutions; algorithmic transparency; open source platforms and algorithms; crowdsourced ratings of contents; but if things like ranking algorithms are transparent they are more easily gamed; tracing content as it flows through the internet - who created it? how was it modified? how do I easily find what people are saying about it?; Need to bring back some sort of data curation (can you do this in a way that isn't biased)
67	Lost tribes can find each other online	Malicious actors can exacerbate social division by linking extremist groups together; small interest groups can find each other and share information, network	Both	We don't know who are building the communities. Exposing the malicious organizers in some cases may be useful. Individuals need to be diligent about rooting out the trolls from online communities so malicious actors can't radicalize them. Need Americans to care that Russians and foreign actors are manipulating the information space, even if the message they are pushing aligns iwth their beliefs Need to provide people graceful exits from the information positions theyve bough into so they don't dig in further- non confrontational messages
68	Open networks	Anyone can message anyone	Both. The problem is that people gravitate to people who confirm their beliefs/ values	Bots and AI can help expose people to alternative ideas, indicate when people are tuning into too much bias, help expose alternative sources of information Anonymity is a benefit for human rights activists and idssidents in foreign countries; but in free societies it can be detrimental; imagine if you walked around Phoenix and half the people were wearing masks. Would you feel safe? We need to acknowledge there should be different rules in different societies based on their legal systems; the more likely it is that they will be persecuted the more they need anonymity
69	Anonymized networks	Information/Messaging can be put out without fear or reprecussions	Both	Anonymity is a benefit for human rights activists and idssidents in foreign countries; but in free societies it can be detrimental; imagine if you walked around Phoenix and half the people were wearing masks. Would you feel safe? Do we need to acknowledge there should be different rules in different societies based on their legal systems; the more likely it is that they will be persecuted the more they need anonymity. What's the greater threat? Do we want anonymity even if it destroys US society? Or do we give up anonymity and find other ways for activists and dissidents to work? Maybe we allow anonymity in small communities but don't allow it for public "broadcasts"
70	Secure networks	Private conversations are enabled; but criminals and malicious actors can operate without law enforcement being able to monitor them	Both	Promote them. Privacy is crucial. Law enforcement needs to find other means to get information.
71	Dark web	facilitate bad behavior, but also could facilitate privacy, rights activism, etc	Both	Similar to the anonymity network above, but the difference is dark web sites aren't broadcasting, so we shoudl allow anonymity

72	Propaganda is engineered by smart people	Makes it a very hard problem to solve	Negative	How do we discourage smart people from doing this? Educate the target audience so they aren't succeptible to manipulation; start in kindergartend
73	Memes	Can persuade easily often using non-verbal images	Both	Education is the key
74	Anonymitiy enables bad behavior	see above	see above	see above
75				
76	Some people are unwitting cooperaters in disinformation	People can dig in and not want to change their positions	Negative	Education is the key; give them a graceful ocgnitive exit
77	Algorithms are optimizing	Algorithms can exacerbate filter bubbles; get people addicted to apps and websites; can give you information you really want; generate lots of revenue for companies; Algorithms are good at the status quo, they are bad at exceptions because they're good at recognizing patterns;	Both	Algorithmic transparency; more consumer algorithmic choice; stop optimizing for $$$; You could train an algorithms to find exceptions and find black swans
78	Coordinated manipulative activity is in marketing, politics, and malign people	Two paths 1) don't allow anyone to use coordinate manipulated activity; 2) allow all of it and work with that environment	Both	Internet should be a public utility and you ban coordinated manipulated activity; Create a pay for use model for Facebook that protects user information
79	Propaganda is not new; so what has changed?	More people can produce propaganda; tools enable broader, faster dissemination at less cost; Anyone can mass transmit propaganda; information proveance is non-existent.	Negative	See anonymity
80	US defines war differently than adversaries	Information operations in the US are not as valued as kinetic warfare		
81	Internet is borderless but our international system is based on soverign borders	International law is based upon the Westphalian nation-state model and physical boundaries	Negative	International policy needs to be updated to account for the new (virtualized) world.
82	DIME model of national power - individuals have much more power	Econ- private companies have huge power; bitcoin disrupts currencies; individuals can conduct global information operations; companies conduct diplomacy; individuals can negatively impact diplomacy	Negative	International policy needs to be updated to account for the new (virtualized) world.
83	Emergence of virtualized transnational organizations (eg BitNation)		Both	How do the instruments of national power affect virtualized nations? What does military power mean to a virtualized nation?
84	Conspiracy theorists and extremists use nominal discussions about things like immigration to inject messages/ shape conversations around racism, sexism, etc			
85	Individuals now conducting hybrid operations with mass shootings, media campaigns, trying to spur leaderless virtual movements	Content needs to be pre-created and staged prior to the event		
86	difference between disinformation, misinformation, and malinformation			
87	Some information is just low quality not necessarily disinformation			
88	Content can be easily tested with mass audiences			
89	Video can now be convincingly and cheaply modified			
90	Bots are used for amplification			
91	Different types of accounts/strategies depending on intent: Bots (amplification), Parody/Spoof (Message testing), Camoflauge/Deep Cover/Account Takeover (Message delivery)	Hard to differentiate legitimate information from misinformation	Negative	Disable anonymity
92	No graph theory models to account for prevailing characteristics of social media networks as opposed to social networks	Scale-free networks explains networks in which the prevailing characteristic is link formation. It does not account for link expiration or link breaking (the primary characteristic of social media networks) which account for self-radicalization and confirmation bias.	Negative	Data provenance and public education.
93	Anybody can mass produce information;			

Slot				
Group Members	Black Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	"Weaponized paranoia" is a real threat	People are getting more aware, but it's also Increasingly sophisticated on the practce	Positive - people more aware that this is an issue. Negative - bad actors are getting increasingly sophisticated. Where is real education coming around this? Possibly may erode science and democratic institutions	Use tools, people, technology to identify early - what is misinformation? Leverage technology to identify it. Need education, critical thinking throughout population
2	Using information deliberately to influence: misinformation, disinformation, malinformation	How do you identify right information vs. disinformation	Positive: more attention in figuring Negative: Need more trained workers to find and stop bad behavior is toxic. Rise in mental health challenges.	
3	New ways to sift through analysis of information (AI programs, more off the shelf options)	Who designs the programs that sift the information? How do we know it's accurate? How do you make the algorhims fair and open (FAIR ML)	Negative: How do we determine what is "fair"?	
4	Track disinformation campaigns to study and categorize the type of disinformation campaigns			
5	Information wars on 2+3 main threats: China & Russia; North Korea, Iran, violent extremism	Move from weapon systems in tradition sense, to information systems. Who is leading that? What is the strategy?		
6	Platform agnostic - many types of platforms and media that it can go through	Quick and dynamic. Can spread from anywhere and to anywhere		
7	Integrated attacks - information designed to trigger action designed to get more media and recruit more actors	It can be sourced and scaled from anywhere	Harder to identify what's real and what should require qction. What do you pick to counter?	
8	Immediate amplication through toxic ecochambers (use to amplify disinformation)	More you let it go, the dangerous it becomes	How do you balance regulation with free speech?	More regulation (self regulation or govt) to identify and take extreme views off the platform. Investigate business models around extreme behavior
9	Traditional warfair being applied to infomration: Techniques, Tactics & Procedures		Do all countries regulate by the same values?	
10	Cyber-forensics used to discover bad actors on the web to discover coordinated attacks	Need to find people who can create programs to stay abreast of tactics and local cultural context (language is key!)	Negative: where will the talent come from?	
11	Meme-factories generating disinformation	What makes memes go is how well it gets absorbed. How it gets adapted. In closed societies, they are using symbols to get around censorship (rice + bunny rabbit for #metoo)		
12	More disinformation campaigns impacting more sectors (elections, corporation reputations, etc.)		Who is the watch dog?	New standards need to get created? Who is the watch dog
13	Rise of deep fakes			
14	Increased investment - public and private funding to fuel and combat the issue			
15				
	Weaponized paranoia is far more suffisticated, wide spread and well coordinated than in the past. Quickly moving from era of online to offline, where people take action, and have attitudes/behaviors influenced based on the			
	information/influence from the information environment. Violent extremism is consistent reminder of this...dangerous when influence is acted upon.			
	- Where is the talent going to come from to address this? Corporate talent, government, defense industries.			
	- Who regulates? Where does the new "standard" come from...established and enforced by who?			
	How to continue to ensure "consumption awareness" - critical and "slow" thinking of information			

Slot				
Group Members	White Chip			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Hard to descern misinformation and disinformation	in order to know facts you have to investigate multiple sources, and shorter attentional span and overwelming data makes a single individual might be interesting in digging for the truth. Only really care if it is entertaining, but fact based narrative is not required. Distrust of fact based scientific narrative that cannot be experienced.	Negative as very hard to show bad behavior and also hard to prove validity of soures or arguments. (The Death of Expertise) the digitialize of online sources and broad availailbity of information lets all become experts. Still takes time to ingest data. How do you acknowledge experts. Involvement of experts in false narratives discredits experts. Deligitimization of these experts.	
2	Friend cycles and preferences and invovlement in choosing	Diversity of Friends and friend groups causes the Z to discredit experts and "think tanks" and as a result will not provide the market as they walk away from the nonexperiential learning with high bar to entry.	We have brought them into the decision making process and will expect to be included. The deffernce to experts is going to be problematic.	need to have think tanks, educational institutions to have transparent funding reports to trace the funding and establish the ligitiamacy and bias of funding. Need to engage in countering misinformation to show the real value of experts. They must provide solid, scientific based arguements and aggressively discret false information. Not enought to prove the point, need to also address dirstractors or differing opinions.
3	Online Friends are Real	trust element in the internet	Skills to identify online charlatans and in person are different. However, we have to admit we have met people in real life that were trying to decieve us or market to us.	
4	Working for good and value of fairness	project fairness onto others on the internet and reject the idea that others would be trying to deceive them for naefarious reasons.	Will probably not project across cultures. VContactia and other russian media are different and discimating the false narratives aggressively for their own purposes. Campaigns have to address the impact on the social good or create the alignment with the social.	Important to be looking at across cultures and platforms to track and enforce across the russian networks. Similiar to UN need to be created to regulate Facebook, it cannot be just be ruled by US Law. A new design of thinking of companies vs countries. Beyond Westfalia.
5	Experiential Learning on and off line, and participate in the narrative	can't control how the experiences are constrained,difficult to get different opinion	Lack of normative causes them to distrust everyone, but trust themselves. The volumne of variety of narratives and truth gets disregarded.	Not enough to just put fact based information into the public square. Need to explain why they need to value a particular piece of truthfull infomration. We need to establish new metrics of trust and find ways to teach both what is right as well as incorrect
6	Their resources are online, mulitute of public squares online	They will look for diversity of opinion on the internet as a part of their explortion but it is very hard with architures of internet to break into differnt thoughts. Russian propaganda is also online but in different forums so you will not find them if you are not on those networks.	Believe that the resources reflect the entire world, but are really only a fraction.	Babel Fish type technologies to have real time translations across language barriers to facilitate a truly global perspective.
7	Enjoy reflections by friends on these they like, not on same tools as the other generations. Utube Channels and peers networks	Reinforcement of bias and huge amount of information availalbe to confirm their biases. The ability to spend huge amounts of time on one topic limits the time to absorb the breath of society and issues across society.	Positive if you can influence the peer groups, and will be equally difficult for all narratives.	Need to find ways to convince influential members of peer and get these influencers to replace the role of experts and authority.

8	Many tasks so work to complete to get to next - speed of injestion	A huge amount of stimuli can mask lack of depth	Impression bias and clickbait type informtion can cause messages to be transmitted unintentially and operating at the same speed as information is critical.	
9	Tools are always on so need to finish now	Increase of stress for tasks that cannot be finished quickly, hard to keep the huge list of pririties that need to come back to and attempt to finish. Expect to be able to participate however, whenever and whereever they desire		how do we create the scaffolding to allow the information to stick and also have the informaiton when it is requested.
10	Diversity among Z and between millentials	How do you educate and inform such a diverse population that are coming with such a diverse backgrouds as well as interests. Will walk away if not invovled, but need multiple narratives to engage across the society,	Develop of the message/narrative can take longer than the "news cycle" causing the truth to be shooting after the duck.	Method as well as the product becomes very important. If you choose and succeed with the audience, you still only have a small part. Levels of differsity and interestes are consistenty changing.

Slot	Brad Schneider			
Group Members	Black Chip			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Diverse: demographics, preferences, likes/dislikes	Contributes to **fragmentation across society** (but isn't the main driver of it); also: hopeful and idealistic; forcing traditional organizations (i.e. churches, universities) to relook traditions of acceptance	positive	Either increase tribalism & fragmentation OR increase inclusiveness at potentially the cost of maintaining traditions
2	Given powerful digital tools "digital natives"	Borderless world - may be providing basis for nativism and xenophobia; sexual contact starts later, but exposure to pornography is earlier and more intense —> easier to isolate self than create relationships; physical geography matters less	negative	Encourage non-geographic similarity and connection; must consider the implications of a technological fix
3	Universal acceptance	Also seeing a **rise in identity politics**	positive	Generate support from large geographically diverse groups
4	Expectations: participate whenever, wherever, however	If there are products w/o experiental expectations - leave or create own; relying on own experiences is a cognitive bias which leads to easier acceptance of tribal narrative; "Truth," "Belief," "Acceptance," and "Identity" are different	negative	Opportunity to drive people off products (or platforms) or towards products (or platforms) based on participatory expectations; opportunities to "detox" or take a break from tech
5	Marketing and product-oriented organizations control the technology	Limiting or controlling the tech is not viable; too many interests; dual-use with positive/negative uses; whole of society contexts make it useful for many different domains	negative	
6	Participatory parenting	Conservative person tends to more authoritarian parenting style —> specific to class structures and world view; more liberal person tend to more participatory parenting style; context of course matters;	negative	Cutting off from mainstream culture (i.e. home schooling) due to threat that kids are being influenced too strongly
7	High stress dealing with own youth and adult situations	High stress **relies heavily on heuristics** (i.e. one's "narrative") rather than "system 2" rational analysis; External manipulator can use this info and fear, anger, other powerful behavior drivers to move to action	negative	add delays into the system, so the cortisol responses drop
8	Committed to equity and own family finances	"Equity" is a trick word —> to libertarian, equity means keep what you earn; to others, (egalitarians) equity means sharing amongst all;	positive	
9	What is impact of older generation?	Lack of "adult" mentorship; use of "adult" organizations to **communicate to next generation** (builds "tribal" societies); victory of Rosseau over Voltaire	negative Transition to US tribalism may have future benefits akin to other tribal structures	form interest-based connections across generations
10	Perspective from privileged American gen Z	Brains develop differently ; two-tiered culture (access vs non-access)	negative	form interest-based connections across priviledge/non

Slot	1			
Group Members	Blue Chip			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Children born after mid-90s are most diverse in terms of friend circles and preferences. Both societal values and because of the digital tools available	(Assumption: valuing diversity means diversity within social circles) - This suggests that there is more potential for people to be exposed to view points and experiences different from their own	Positive	1. Create a campaign that leverages this trend in Gen Z as a motivation for the older generations to do the same thing. 2. Campaign targeting Gen Z to encourage expanding beyond diverse social circles into valuing discourse
		(Assumption: valuing diversity means that the differences between social circles is greater) - this suggests groups are getting smaller and the distance between them is increasing	Negative	1. Campaign targeting Gen Z similar to early 20th Cent to encourage activities that are social good (meeting other people, engaging in discussion) ref Heinekin ad about building a bar
2	They expect to be able to participate in all the data sources (cause, film, game, etc...) they have access to and want to be able to participate in a number of ways and situations	The communication that wins isn't just based on the message, it is also based on the medium that lets Gen Z interact in the ways they want. Which means merit of message is less important than sophistication of medium (which biases for money and resources) and less important than accessibility (the more ways you deliver the message the more likely you are to win - Baader Meinhoff phenomenon)	Negative	Come up with multi-modal methods of communication rather than old fashioned PSAs/websites. Personalization; target audiences need to be able to relate deeply.
3	They are more stressed due to their parents sharing more about what is stressing them	Gen Z is indoctrinated into high stress world views at a very early age, which makes it hard to get them to even start to think about how to question those views	Negative	This is not really new, parents always indoctrinate their children. Focus on education around critical thinking
		The childish behavior (sharing of weaponized memes, etc...) of parents is now much more visible to children due to them being on the same social media platforms	negative	**Ad campaigns targeting parents to stop role modeling this behavior - this generation's version of "I learned it from watching you dad!"**
		Children that grow up watching their parents spreading weaponized memes will think there's nothing wrong with having political leaders who behave that way and in fact may prefer it	negative	1. Focus on education, setting examples and role models of what good behavior looks like - (ala sex ed, stop smoking). 2. Create policy that prevents echo chambers
4	Very committed to causes, more serious, understand hard work	Everything they are commited to is utterly critical to saving the world (regardless of political leaning). They are much more likely to be tribal	negative	Create more opportunities for cross-group collaboration
		They have the potential to do great things and to lean into things that are uncomfortable	positive	1. Create more opportunities for cross-group collaboration. 2. Use social media to amplify spaces for constructive collaboration **3. Drive the concept of self-policing; communities are responsible for holding their most extreme members to a standard of good behavior that they would want to see from the other side**
5	They value diversity and want to create more equitable society & environment	Given the opportunity they might be willing to actually voluntarily do work to make this happen	positive	Create a public service program for people to participate in creating positive environments
6	This generation has never had "no access" to the Internet			
7	This generation has had social media from the start			
8	World wide this gen pays attention to what is coming out of Silicon valley and don't want to be left behind			
9	This generation has had the war on terror for their entire lives			

10	People gain their identity from their groups and we are seeing more fragmentation into smaller and smaller groups			
	https://twitter.com/alexstamos/status/1091710534804594688?s=21			

Slot				
Group Members	Green Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Censorship	Is this too broad of an issue?	Can be either	
2	Cognitive Ease	entice people to self-reflection, and then engage with learn, and potentially embrace new truths?	Neither	If you want to start a revolution, throw a better party.
3	Confirmation Bias	People on all sides virtual signaling, the internet as a mirror of both the society we live in an the identities we wish to fortify.		
4	how to make people care about	throw a better "party" to entice		
5	the internet as a mirror	Distorted reflection as a hall of mirrors - opportunity to amplify certain divisive features, perpetuate them, threaten/exclude other perspectives	Both	As internet become more integrated into society, internet less of a mirror because becomes and extension of individual selves - As becomes more integrated, less ability for anonymity
6	self harm/otherize	Self-destructive behavior is no longer *self* destructive in a connected word.		
7	so much of democracy is about the process of contesting knowledge. it works when we're able to have a healthy media/knowledge ecosystem. the fact that so much communication happens out side of the view of media	Ease of access to constantly-present information		
8	things are subtle:memes, not quoting sources, complexity of language, signals&signaling, rhyming as away of signaling meme, playground bullying with machine learning, signals get the confirmation bias going	Journalists, fact-checking, and knowledging contesting / synthesis breaks down. If '90 percent' of human communication is non-verbal, what's the non-verbal communication equilivant of online.		What's the immune system for toxic signaling and non-verbal communication and behaviors. What's the relationship between signals, and behaviors? You could argue the best influence attacks are based on hidden or explicit signals that get past a) algorithmic detection b) journalism oversignt, c) community immune systems to disinformation
9	How to get tone in text, could you identify when someone wants to start a fight, e.g. ends with a period	People defer based on subtlties in real life (appearance, gender, height, percieved authority) - have we identified what causes people to defer authority online? Can that be utilized as the subtle way to promote self-reflection?		
10	what's the non-verbal in digital communication			
11				

12	Determining a need for censorship and regulating potentially increasingly-radical conversation/thought			Our Design Victory Condition is to render censorship unnecessary? What's the healthy, non-authoritan digital panopticion? How do we reintroduce, non-extreme, human level consequences, build family and community connect and empathy, and deter toxic behavior. Lots of little sub-conscious corrections, you don't have to internalize and take it personally, or have it feel like an attack. De-escalation, healing, re-connection to the community are built into the correction in ADDITION to accountability. This happens at the individual level, as well as groups within a community (which probably requires a similar, but different kind of reconciliation, negotiation)
13	Tunnel vision, desperation in the face of change	need to protect homeland, need to sustain self (economically, socially), respond to state-based/non-state-based narrative attacks		principles-based approach to information warfare; defending definite truths - promoting democracy vs defending democracy and deciding on whether to adopt multilateralism

Slot				
Group Members	Purple Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Lack of transparency	People have the right to know who's whispering in their ear		policy, police the hell out of the platforms to be transparent
2	media and platforms as business	Business model of maximising clicks and ad revenue drives content that is not necessarily journalistic of balanced		regulation of platforms or education of consumers?
3	censorship	Balance of freedom of speech and control		regulate platforms and culture of conversation, not content; self-regulation of communities (platforms that give more ability to self-police, assert rules)
4	critical thinking, education	critical thinkers, media literate audience knows to ask "why"? perpetual learning; constantly reinventing the quality of public discussion		education (discussion, debate); open discussion space and culture; role of good old investigative journalism, the least profitable part of the medi business;
5	peoples preconcieved notions, tribalism, identity politics	A lot of public communications is based on stereotypes and in-groupism		
6	targeting the enemy with tools we cannot target our own people with			
7	Information segregation, information bubbles	Creates echo chambers; feeds confirmation bias	Negative	
8	extremist content (ISIS, etc.)	Insighting violence in the public sphere	Negative	transparency, notice and takedown
9	attention economy	attractive content is on the shallow end		stop payng attention to the extremists; educating an audience to be demanding
10				

Slot				
Group Members	Grey Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Didnt make correlation between narrative and confirmation bias	not clear how cognitive bias plays out	both	identify how confiermation bias promotes esisting narrtives; elaborate additional cognitive biases that might impact narrtive acceptance
2	which narratives more likely to be effective	resource allocation; amelioration strategies		examine the role of emotion; examime the role of communities/bubbles
	can't change the mirror	have to offer replacement if taking about previous narrative; cognitive ease = must make alternative as easy to digest more desirable explanation for the world	negative	re-tool messaging away from "you are wrong" to "here is why the alternative benefits you"; also, make that replacement message easy to disest.
4	botox is a limited treatment	correction has a role	both	better understand which messages are most dangerous (and craft direct counters); identify which narratives are better innoculated with alternative narratives
5	Potential for the cure to be worse than the disease	Dealing with misinformation may be better than changing a foundational American value (1st Amendment/Freedom of Speech/Access to Information	negative	Compare the risks of allowing misinformation campaigns to continue with the consequences of limiting speech/access to information; monitor the impact of private actors limiting speech and/or preventing access to platforms (Alex Jones, InfoWars etc.);
6	what if I dont want to look in a mirror	many people feel disinformation a problem, but most won't correct their biases; most people think that misinformatiion is problem for *other* people	negative	educate the next generation on good information hygeine;
7	I do not like the man. I need to get to know him better	Bubbles are a major part of the current problem -- a broader community of sources helps protect against biases	positive	Encourage news consumers to draw from a borader range of sources; promote mediated/curated discussion across online communities
8	trust is super important	people are more likely to believe a friend than a news reporter	both	news institutions need to rebuild trust; amelioration strategies must leverage grass-roots energy
9	which narratives more likely to be counteracted	resource allocation; amelioration strategies		examine the role of emotion; examime the role of communities/bubbles
10	social wedge	We want people to leave bubbles of social media, however is higher education becoming a problem? Controversial thinkers being pushed out of institutions as they are making students uncomfortable. We are training minds early on to opperate in bubble	negative	institutional awareness of differing intellectual thought as aide to stufent minds. Socratic method

Slot				
Group Members	Orange Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Who is the arbiter of veracity?	Democratic action requires an informed citizenry, so accurate information is a public good, but at the same time free speech is a cherished, national-identity-forming value, which puts into tension establishing an entity for vetting information accuracy vs. stifling free speech	positive and negative	Provide some easily digestible information provenance to help people verify information. People have to care that they are being gamed, before they can begin to fight the problem. Some people are blissfully ignorant; some people have bigger problems than to care about the existential threat of misinformation. People think "the media" are at fault. Truth is socially constructed, so it is not unconditional. Where is the common value?
2	socio-economic drivers of generational perspective (what's important) and values	today's Gen Z'ers and Millenials have a different economic outlook and that drives new values (sharing economy vs. private property ownership) and potentially drive perspectives on the value of socio-political institutions (education, press, govt) as beneficial	risk, with potential negatives; society in change is susceptible to mis/disinformation, disruption	need resilient institutions and adaptive to societal change that acknowledges how people operate in today's world and what they care about.
3	privacy is changing	used to be that there was a specific difference between private informatioin and public information; public spaces and private spaces; separation between public/work, public and social, private and social, private/family, etc; --now those borders have eroded both by virtue of the intrusion of media/social media, and by reconceptualizations (and exploitations) of what is personal/private/public	comes with risk	we need greater awareness of the changing nature of privacy; how do you develop empathy online with only screen-based cues?
4	off shoring of critical infrastructure--pharmaceutical, manufacture	foreign adversaries it can be used for social credit or other means of exploiting citizens; can disrupt institutions and exploit fear.	comes with risk	secure supply chain with blockchain or other tools
5	off shoring of critical infrastructure--technology talent	foreign adversaries it can be used for social credit or other means of exploiting citizens; can disrupt institutions and exploit fear.	comes with risk	
6	increasingly complicated nature of (nearly every) aspect of society from health care to economy, etc.	rise of populism: sweeping, simplified, emotional arguments to bucket a range of complicated problems into a simplied 'solution' that is really simply a route to power consolidation by the perpetrator of the simplification	comes with risk	
7	education			
8				
9				
10				

Slot	1			
Group Members	Brown Chip			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Flawed analysis that got us to the discussion of GEN Z.	The perceived power distance between GEN Z and older generation is an actual reality vs belief.	Initial reaction across the board is negative for all of these data points and implications however we have not fleshed out.	Drink a beer!
2	Protests challenging DoD working with corporate America. The generation should influence what projects their companies undertake not just what individual projects "they" undertake.	1% of the population having experience with the DoD. How does the DoD stay on the forefront of the free world when an inherant distrust is present to what the DoD does.		
3	What drives these technological companies? Generation Z has more leverage with these companies. Their work will have impact not two years from now but two weeks from now.	Is it money, is it resources or is perception that drives these companies? To what extent is their a tension of a company that its purpose is to make money vice provide greater good to the community? Global companiys (perponderance of US companies) are driven by GEN desire. Compromise maybe the true driving initiative. Company is optimizing not soley based on profit. The compromise on the bottom line vs other values.		
4	GEN Z willing to work hard but need to see immediate impact.	The need for physical communities will diminish. Perhaps the pressures to hold them together is diminishing or becoming harder	Negative	
5	Active roles in political and social activities.	Equity issues of relationships as employees of a company vise GEN Z ers as consumers of society. GEN Z will not give up things like Twitter even though it has some of the most hateful and divisiness present.		
6	Millenials and GEN Z will be 75% of the workforce...WOW!			
7	Technology is disaggregating society.	The amazon example driving companies to certain methodologies... shipping to home vs travelling out to purchase things.		
8	The Industrial Revolution made the US what it is but the US is no longer in that econmic state.	Institution are inadequate to address the present much less the future and will brake the paradigm.		
9	Any place, Anytime, Anyway			
10	Self organization takes place now in cyberspce because of the limits of the terrestrial space.			

Slot	Ben Decker			
Group Members	White Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	malinformation is true, disinformation is false			
2	meme is something that spreads like a disease vector; what's new is memes that cause action in the real world.	memes do not require literacty -- can be consumed as cat videos		
3	dependent on receptive audiences			
4	digital landscape/terrain			
5	amplification/manipulation			
6	testing at scale/speed/rapid feedback loops			
7	influence/interference			
8	"platforms" content/atomic unit			
9	diffusion			
10	adversarial behavior intent	divide/polarize		
	what happened when people decided that gay marriage was okay?			
	everything you thought you knew was wrong events	speed that these events happens		
	what happened when people decided marijuan was okay?			
	2nd and 3rd degree implications of current influence operations			
	75% of the workforce is going to be gen z and millenial			
	impact of deep fakes?			
	can the chaos creators open to attack by their own people?			
	can the muslims attack the chinese regime?			
	Assume the tools to create all forms of media effectively have become ubiquitous: ai, augmented reality, deep fake videos, games, movies, media platforms, social networks.			
	Audience Receptivity: Gen Z example of having media everywhere in multiple forms? And how that effects our values and ethics? Synthetic vs. Natural, Transcending our digital space,	A new set of values, a cultural revolution to a spiritual revolution, against the tyrannies that seeme inevitable --suppose there is a reaction to all the things that are scaring the shit out of us to one that is focused on ethics and values...people are looking for bedrock. A spiritual revolution. A mass movement towards real.		
	ethics? values?			
	What is the path to everything you thought you knew was wrong event?			
	What are the TTP's to piss on things we know now that are wrong?			

Slot					
Group Members	Blue Pawn	https://www.demdigest.org/wp-content/uploads/2018/08/disinfo-Types-of-Information-Disorder-Venn-Diagram.png	https://medium.com/@jamesbridle/something-is-wrong-on-the-internet-c39c471271d2		https://www.amazon.com/Death-Expertise-Campaign-Established-Knowledge/dp/0190469412
#	Data Point	Implication	Positive or Negative?	What should we do?	
1	Post-Truth Society	Tribal truths rule			**Positive**
2	Online social media platforms	Easy to connect and amplify, weaponize			Democratic
3	Conspiracy theories	Persistent alternative interpretations of reality and who is in control, narrative trumps truth			Secure
4	Faux insiders	Creation of a false credibility base, appealing to emotions			Fair
5	Alt identities	Bots, fake IDs, malicious actors			Pursuit of Happiness
6	Troll farms	Industrialized astroturfing and grassroots propaganda			
7	Propaganda for all	Anyone can propangadize, does not require state-level resources			
8	Cross-border interest groups	Digital tech allows interest groups to act globally			
9	Radical levelling	End of expertise, anyone can speak out, democratized voice and participation			
10	Editable history	Blur truths, revisionism			
11	Accelerationsim	Speed up events			
12	Millenialism / Apocalyptics				
13	Social Fragmentation	self-imposed segregration?			
14	Hybrid State Warfare				
15	Ideology over epistemology				
16	Globalization favors closed societies	Open societes are vulnerable to state-sponsored bad actors			
17	audio/video/Photo manipulation	Easy to manage perceptions or edit reality			
18	Revolution rhetoric				
19	Chaos is a ladder	Fomenting chaos creates opportunities for excluded populations			
20	Crisis Opportunism				
21	Who is the threat actor?				
22	Funded, coopted media	narratives reinforced / transferred into the mainstream / enhanced credibility			
23	Technology ignorance	Tech savvy people can manipulate the ignorant			
24	Gambler doubling down/sunk cost falacies				
25	Long term effects of weaponized narrative (algorhithm based childrens videos)				
26	2020 is going to be a mess				
27	Narrative Trumps Reality	the end of expertise, a society needs a shared narrative to exist	Both		
28	People are hungry for authority	Absence of credible authority (idols) creates opportunities for multiple sources of truth	Negative		

Slot				
Group Members	Red Pawn			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Information/disinformation is platform agnostic	Easily accessible anywhere; information/disinformation can jump platforms; solutions often platfom specific;	Positive - lots of channels, lots of diversity, lots of options; Negative- disinformation is very hard to combat; no single solution	Platforms should do risk modeling and collaborate on solutions; algorithmic transparency; open source platforms and algorithms; crowdsourced ratings of contents; but if things like ranking algorithms are transparent they are more easily gamed; tracing content as it flows through the internet - who created it? how was it modified? how do I easily find what people are saying about it?; Need to bring back some sort of data curation (can you do this in a way that isn't biased)
2	Lost tribes can find each other online	Malicious actors can exacerbate social division by linking extremist groups together; small interest groups can find each other and share information, network	Both	We don't know who are building the communities. Exposing the malicious organizers in some cases may be useful. Individuals need to be diligent about rooting out the trolls from online communities so malicious actors can't radicalize them. Need Americans to care that Russians and foreign actors are manipulating the information space, even if the message they are pushing aligns iwth their beliefs Need to provide people graceful exits from the information positions theyve bough into so they don't dig in further- non confrontational messages
3	Open networks	Anyone can message anyone	Both. The problem is that people gravitate to people who confirm their beliefs/ values	Bots and AI can help expose people to alternative ideas, indicate when people are tuning into too much bias, help expose alternative sources of information Anonymity is a benefit for human rights activists and idssidents in foreign countries; but in free societies it can be detrimental; imagine if you walked around Phoenix and half the people were wearing masks. Would you feel safe? We need to acknowledge there should be different rules in different societies based on their legal systems; the more likely it is that they will be persecuted the more they need anonymity
4	Anonymized networks	Information/Messaging can be put out without fear or reprecussions	Both	Anonymity is a benefit for human rights activists and idssidents in foreign countries; but in free societies it can be detrimental; imagine if you walked around Phoenix and half the people were wearing masks. Would you feel safe? Do we need to acknowledge there should be different rules in different societies based on their legal systems; the more likely it is that they will be persecuted the more they need anonymity. What's the greater threat? Do we want anonymity even if it destroys US society? Or do we give up anonymity and find other ways for activists and dissidents to work? Maybe we allow anonymity in small communities but don't allow it for public "broadcasts"
5	Secure networks	Private conversations are enabled; but criminals and malicious actors can operate without law enforcement being able to monitor them	Both	Promote them. Privacy is crucial. Law enforcement needs to find other means to get information.
6	Dark web	facilitate bad behavior, but also could facilitate privacy, rights activism, etc	Both	Similar to the anonymity network above, but the difference is dark web sites aren't broadcasting, so we shoudl allow anonymity
7	Propaganda is engineered by smart people	Makes it a very hard problem to solve	Negative	How do we discourage smart people from doing this? Educate the target audience so they aren't succeptible to manipulation; start in kindergartend
8	Memes	Can persuade easily often using non-verbal images	Both	Education is the key
9	Anonymitiy enables bad behavior	see above	see above	see above
10				
11	Some people are unwitting cooperaters in disinformation	People can dig in and not want to change their positions	Negative	Education is the key; give them a graceful ocgnitive exit
12	Algorithms are optimizing	Algorithms can exacerbate filter bubbles; get people addicted to apps and websites; can give you information you really want; generate lots of revenue for companies; Algorithms are good at the status quo, they are bad at exceptions because they're good at recognizing patterns;	Both	Algorithmic transparency; more consumer algorithmic choice; stop optimizing for $$$; You could train an algorithms to find exceptions and find black swans
13	Coordinated manipulative activity is in marketing, politics, and malign people	Two paths 1) don't allow anyone to use coordinate manipulated activity; 2) allow all of it and work with that environment	Both	Internet should be a public utility and you ban coordinated manipulated activity; Create a pay for use model for Facebook that protects user information
14	Propaganda is not new; so what has changed?	More people can produce propaganda; tools enable broader, faster dissemination at less cost; Anyone can mass transmit propaganda; information proveance is non-existent.	Negative	See anonymity
15	US defines war differently than adversaries	Information operations in the US are not as valued as kinetic warfare		
16	Internet is borderless but our international system is based on soverign borders	International law is based upon the Westphalian nation-state model and physical boundaries	Negative	International policy needs to be updated to account for the new (virtualized) world.
17	DIME model of national power - individuals have much more power	Econ- private companies have huge power; bitcoin disrupts currencies; individuals can conduct global information operations; companies conduct diplomacy; individuals can negatively impact diplomacy	Negative	International policy needs to be updated to account for the new (virtualized) world.
18	Emergence of virtualized transnational organizations (eg BitNation)		Both	How do the instruments of national power affect virtualized nations? What does military power mean to a virtualized nation?

19	Conspiracy theorists and extremists use nominal discussions about things like immigration to inject messages/ shape conversations around racism, sexism, etc			
20	Individuals now conducting hybrid operations with mass shootings, media campaigns, trying to spur leaderless virtual movements	Content needs to be pre-created and staged prior to the event		
21	difference between disinformation, misinformation, and malinformation			
22	Some information is just low quality not necessarily disinformation			
23	Content can be easily tested with mass audiences			
24	Video can now be convincingly and cheaply modified			
25	Bots are used for amplification			
26	Different types of accounts/strategies depending on intent: Bots (amplification), Parody/Spoof (Message testing), Camoflauge/Deep Cover/Account Takeover (Message delivery)	Hard to differentiate legitimate information from misinformation	Negative	Disable anonymity
27	No graph theory models to account for prevailing characteristics of social media networks as opposed to social networks	Scale-free networks explains networks in which the prevailing characteristic is link formation. It does not account for link expiration or link breaking (the primary characteristic of social media networks) which account for self-radicalization and confirmation bias.	Negative	Data provenance and public education.
28	Anybody can mass produce informa			
29				
30				
	Top level points			
	Anyone can produce mass influence campaigns			
	Anonymity is problematic			
	We need to run the Internet as a public utility; need a for pay model for Facebook			
	Graceful exits from cognitive positions			

Appendix 5

FUTURES WORKBOOK DAY ONE AND TWO

In groups, participants develop scenarios based on data inputs from each speaker. The inputs were randomly selected. These scenarios followed a strict outline designed to envision a person in a place with a problem. Participants answered a variety of questions about their character including, "Describe how your person experiences the threat." In addition to designing future scenarios from an individual character's perspective, groups also explored the experience of the adversary.

Finally, groups were pushed to backcast. This foresight tool defined – what we have control over, what we do not have control over, and steps we should take to disrupt, mitigate, and recover from these futures four and eight years out.

This exercise was done twice, once each day, and the workbooks were used to inform the scenarios, found in this report. Participants had between one to two hours to complete the threatcasting process.

The information found in the following pages is raw data and has not been spell checked or edited in any manner.

FUTURES WORKBOOK DAY ONE

Team Members:	**Black Chip**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Perspective from privileged American gen Z - Brains develop differently ; two-tiered culture (access vs non-access) - negative - form interest-based connections across priviledge/non
Speaker 2	censorship - Balance of freedom of speech and control - regulate platforms and culture of conversation, not content; self-regulation of communities (platforms that give more ability to self-police, assert rules)
Speaker 3	Ideology over epistemology
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Anna is a Cuban, black, lesbian, immigrant, 22 y.o.; brilliant technologist brought in by Space-X; expertise is exo-psychology, or tweaking people's brain activities for members of the Mars colony; NASA is now a subsidiary of Space-X
Where do they live?	Simple, two-bedroom apartment outside Huntsville, AL - part of the Space-X campus
What is the threat?	Community security problem; "One Planeters" wealthy religious fringe group oppose the Mars mission; conducting "low & slow" attack on integrated cognitive interface to disrupt and threaten the mission on the grounds that all mankind should live on Earth; "OP's" goal: collapse of the Mars colony from within (**This event happens: "Everyone on Mars walks outside without suits!**)
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Anna connects daily with a brain interface connected to Mars; she feels some dissonance/uncanny valley with her connection b/c "One Planters" have begun manipulating her worldview and experiences during off-work hours through home-based computer brain interfaces contributing to her social media feeds
What is it? 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?	
	Josie is Anna's girlfriend who is jealous of the time Anna spends time with the colony and the sophistication of the connection with colonists
What vulnerabilities does this expose?	
	Development of meta-cognitive networks highlights new security vulnerabilities (not just technical, but social)
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
	Plan of Attack (in order of escalation) 1. Attack Carol Reptuationally and Politically, if that doesn't work 2. Attack her at Church, when that doen't work 2a. Get one of their children addicited to neurochemically hypnotic Augemented Reality Porn, then leak it to members of the church. 3. Alongside, try and economically seduce George into selling the farm 4. Bring in Carol as mistress to exploit George to steal IP 5. When that doesn't work, cause maximum destruction and chaos by making them get a divorce
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	

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?	Chinese or multinational use the information systems in the church to spy on Lily, and find vectors for gossip and chaos. Church is the attack on Lily begins
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?	Is she going to be able to keep her name? Try and wipe some of her digital identity? Will that make it worse? How does a person not only deal with an identity attack, but how does she rely on her community to heal an influence and reputation attack?
What are the broader implications of a threat like this? What might a ripple effect look like?	
Question One	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	Mars colony mission collapses; Space-X goes bankrupt; Mars exploration abandoned; One Planeters "win"
Question Two	**PASTE HERE**
	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	Anna is the first person to watch the colony walk out the door
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	More is known, more is entangled (business / government connections, the tech and data layers are entangled) in ways that are hard to detect or prevent.
Question One	**PASTE HERE**
	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?
	AI system platforms on her cognition that can look for an incursion; One Planeters supported through back channels with an corporate competitor; hacking the girlfriend's Josie's cognition through her recommendation feeds and what she sees and consumes; "Attack AI" developed to establish reflexive (passive) control of Josie
Question Two	**PASTE HERE**
	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?
	brain-machine interfaces. Adversarial neural networks. Low-bandwidth communications. Brain mapping. Brain-brain interfaces.
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.	

Gates:	
What are the Gates?	Josie's access to Anna; Anna's access to the cognition link; psychologist on Mars; selection of Mars volunteers who are hardened against psychological manipulation;
List out what the Defenders (government, law enforcement, industry, etc) 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	Space-X contractor, DynCorp "watches the watchers"
2	Space-X C-suite
3	
4	
5	
Flags:	
What are the Flags?	Space weather; One Planeter's narrative & recruiting; Other corporate competitors
List out what the Defenders don't have control over to disrupt, mitigate and recover from the threat. These things should have a significant affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team Members:	**White Chip**
Experience Title:	**Preventing Texit**
Estimated Date:	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 Slot)	
Speaker 1	They value diversity and want to create more equitable society & environment
Speaker 2	Balance of freedom of speech and control
Speaker 3	Tech savvy people can manipulate the ignorant
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	A 33 year old professsional Latino Man
Where do they live?	Dallas, Texas
What is the threat?	Texas is holding a refendum to succeed from the United. The white majority alt right and alt left politics have inflamed identity politics and it appears likely that the country will break apart.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	The minority professional tried to balance his desire for social equity, while he is personally privileged yet self identified as a minority and invested in the national economy. Possibly unrest as well as economic impact and repercussion for minorities within Texas, as well as migrate to border states and Mexico.
What is it? 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?	
	Family, peers and economic partners in his law firm, as well as church, which is primary Latina politically/socially progressive Catholic church. Also concerned about clients at the firm. The foreign interferrence creates wedges within the U.S. and looks to break the country into several governing entitites or at least create internal division to create freedom of maneuver within Latin America. Cohesive and unified body politic with emboyed national government and engaged and commited electorate.
What vulnerabilities does this expose?	
	Lack of legitimate national authority and social divisions are causing the repeat of a BREXIT vote, designed by adversaries to divert attention of peer powers.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?**
	Clients request new representation as they no longer trust that their latino lawyer can represent in the "New Texas". Heard from the pulpit the concerns that the community would be looking to leave the US and the Church is concerned about religious freedoms after such a split. Reviewing message boards indicate fracturing the idenity politics and advocated the Latino threat to Texas, as the Catholic church is advocating against succession. The Alt Right has convinved the white working class and elite that this cultural war can only be won
Question Two	**What are the broader implications of a threat like this? What might a ripple effect look like?**
	Pueuto Rico, Somoan, and Hawaiians see that they can no longer trust the US. The environmental extremists in the PNW see a potential to re-envision their utopian evergreen vision. The Mormons look to take pre-emptive steps to secure their postion and rights within the US, and also advocate for additional splintering.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**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?**
	Popularity of the constiutional crisis and the increasing conflict between local and federal authourity. Lack of recognized national experts leads to local and regional media dominating newpaper and TV. Extremist influences sewing fear and division thourgh influence campaign to encite the local echo chamber. The media differences by region facilite the foreign actors malicious information information.
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?**

	The adversay will team up with both alt right and alt left to ensure local devision and also drive wedge between regional powers within the US. Delegitimizing the national conflict resolution system while emphasizing imaginary Mexican across the borders. Require new public and private partnerships to include influencers and work across community boundries.
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	Information, facts and narrative concerning the common benefits of US for domestic and international leadership.
2	Telecommunication infrastucture and networks
3	Provabley Secure and authentic Quantum Communication infrasturture
4	Election finance laws
5	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
1	Bot activity
2	Election Finance limits and contributions
3	Racial Tension within states and within schools
4	community level conflict
5	Public accusations of law enforcement bias
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?	
1	Enhance legitmacy of national authourity
2	Educate the population of the benefits of the national identidy
3	Discredic alt left and alt right
4	Technology to identify algorigm manipulation
5	Prosecute the manipulation and influence operations
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?	
1	Identiy ways to flag misinformaiton, disinformation
2	new conflict resolution to involve and empower the influences, on and off line
3	
4	
5	

Team Members:	**Blue Chip**
Experience Title:	**Kristallnacht as a meme**
Estimated Date:	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 Slot)	
Speaker 1	World wide this gen pays attention to the latest communication trends and don't want to be left behind
Speaker 2	what if I dont want to look in a mirror
Speaker 3	meme is something that spreads like a disease vector; what's new is memes that cause action in the real world.
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	28 Year male old Republic of Srpska
Where do they live?	Republic of Srpska
What is the threat?	Influencer politicians uses weaponized memes to drive their election/popularity and promote conservative/rightest movements backing them. The memes kick off a self-sustaining cycle of violence against minority groups who disagree. This results in a crop of leaders across Eastern Europe, South America, and South Asia who form an informal coalition of states that reject Western democratic values. The United States and UK are weakened and divided, and no longer effectively argue for Western norms. This heightens the threat of ethnic cleansing, terrorist violence against authoritarian states, and inter-state violence due to tensions amonst ethno-nationalist leaders. Russia is the dominant arbiter amongst its block.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Nationalist leader takes power in Serbia; rejects Western relationships in favor of Eastern block; builds power off expoiting Serbian irrendentism
What is it? 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?	
	Parents share memes affiliated with ethno-nationalist groups promoted by government; youth engaged via more radical VK stories, including videos produced by paramiliary groups
What vulnerabilities does this expose?	
	Domination by malign media narratives playing on etnic tensions
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	Sasha is received a meme via a next generation (WhatsApp) -- whatever that will be -- feeding a story of a purported act of violence against a Serbian by an ethnic Bosnian, followed by coordinated calls in social media to carry out violence. This follows a nationalist campaign for Srpska to be annexed by Serbia
Question Two	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	The event could lead to renewed conflict between Serbia and Bosnia, ethnic cleansing, intervention to potentially include "peacekeeper" deployment by Russia, and weak to no response by the West. Memes deployed in the West will target Left (ant-imperialist) and Right (anti-Muslim) populations to attack Western intervention.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	End efforts of Serbia to join the EU; continue weakening of Western tilt amongst Eastern Europe
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?	
Question One	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?
	Acceleration of WhatsApp closed platforms, coopted by government networks
Question Two	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?
	State/parmilitary 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.	
Gates:	
What are the Gates?	

List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team Members:	**Green Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Very committed to causes, more serious, understand hard work
Speaker 2	How to get tone in text, could you identify when someone wants to start a fight, e.g. ends with a period
Speaker 3	"Chaos is a ladder"
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Lily the Farmer (primarily soy), single mother (kids aged 7, 13, 16), small business owner.
Where do they live?	Iowa small town.
What is the threat?	Loss of identity, personhood, and livelihood through corporate espionage caused divorce.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Husband (George) leaves Lily for Carol (church friend, but also daughter of multinational soybean conglomerate executive, who runs a company owned by an international energy company owned by a particular state, and an agent of the foreign government of that state) and abandons the kids, leaving her the (George's) medium-size family farm as compensation. Family farm is called Smyth Soy, after George Smyth's father, which is a stable name in the local community and in midwest farming. Lily is the president of the Iowa permaculture association and is gaining ground as an influencer, presidential candidates consult her. George leaving Lily makes her her growing techniques vulnerable to foreign agents (Carol), reduces Lily's influence and questions her status as a pillar of the community, as a now-single mother and divorced woman. Lily's income relies upon her relationships with fellow farmers, and her income is therefore threatened by Carol. Foreign government wants to ruin her life, get the farm land/IP, obtain her growing techniques and technologies either to utilize for their own corporations' operations or to bury to maintain the status quo.
	Add in tone over text - the entirety of her internet-based interactions with humanity (friends, aquaintances, local HOA, existing and potential customers) change to a tone of implicit dislike, further eroding her psychological health and adding to the 'accepted narrative' that Lily is disliked.
What is it? 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?	
	Husband, Lily's kids, neighbors, fellow churchgoers. The entire brand of the farm is/was based around the small town family dynamic of the husband and wife running a business together. Smyth Soy is technology-dependant. The threat is the mistress (Carol), her access to the intellectual property held by the husband, technologies and techniques used by Lily and George, and the consequences of the husband's actions coupled and expanded upon by the dependence on technology and branding that they have built. The multinational agricultural corporation is seeking to obtain Lily's techniques, technologies, land, and water rights by undermining her character, ruining her business brand, and corrupting her children i.e. ruining her life
What vulnerabilities does this expose?	

	Lily's entire online identity has been built around her roles as a small business owner, wife, mother, and good church-going Iowan. Due to her husband's betrayal, she is considering going back to her maiden name (Johnson), but is concerned about the implications for the name of the farm (re-naming would require massive rebranding) and having a different last name than her children in a small, gossip-y town. Lily's entire income is vulnerable as the multinational corporation seeks to steal her techniques and technologies and she now has to re-build a well-established brand, including shoring up current business relationships, while continuing to raise her kids, who are seven, 13 and 16 years old. Her children are exposed to actions by foreign agents, who seek to undermine Lily and sully her name in the greater farming community.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	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?
	Lily will on the surface primarily see her husband's cheating as a betrayal, involvement / apathy of the church as a betrayal. She will be devastated and after initial period of loss and depression will want to reclaim her identity, likely through re-branding the farm and changing her last name back to her maiden name. She will not see or understand until later that George's betrayal was manipulated by a 'honey pot' foreign agent, Carol, as part of a campaign to discredit Lily and steal her intellectual property. Lily will feel that her income and way of life are vulnerable; her position in the community is threatened; her online personal and business profiles and reputation are under attack by unknown individuals; and her children are teased by schoolmates, excluded by school faculty, and vulnerable to corruption by foreign agents.
Question Two	What will the person have to do to access people, services, technology and information they need?
	Part of Carol's backstory (or convenient coincidence) is her active involvement in the church, she is well liked by the community, and has used Lily's strong (though personable) personality in the public sphere to portray Lily and George's prior-to-divorce homelife as miserable. Thus, Lily struggles in the small town to access resources, as she is ostracized by her community. Her kids recieve some of the backlash as well as collateral damage, as the public percieves (through Carol and the church) that Lily obtained full-custody through coersion rather than George's abandonment. Through interconnectedness and entanglement, the divorce stains Lily's entire personhood, as her online persona is linked to her business to her children to her social life, even bank account and driver's license, etc.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**
	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?
Question Two	**PASTE HERE**
	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	Protections for IP
2	
3	
4	
5	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
1	Personalized online targeting directed at Lily's kids - (hate your parents?)
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?	
1	Efforts to disentangle Lily's personal online persona from public online persona.
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?	
1	
2	
3	
4	
5	

Team Members:	**Purple Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	The Industrial Revolution made the US what it is but the US is no longer in that econmic state. Institutions are inadequate to address the present much less the future and will break the paradigm.
Speaker 2	censorship. Balance of freedom of speech and control
Speaker 3	Chaos is a ladder. Fomenting chaos creates opportunities for excluded populations
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Female, high school, postindustrial, border town
Where do they live?	Yuma, AZ
What is the threat?	chaos caused by, breakdown of economic and therefore social order
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	lack of jobs (structural unemployment) and opportunity, impowerished neigborhoods (lack of services, fresh food, low quality public space, leading to lack of security). This leads to desire for authority, someone to try to fix it as well as public health crisis. Uncertainty leads to overthrow of government, breaking down food supply chain. Martial law and isolationalism. Border wall is digital but with tunnels underneath. US citizens occasionally cross to Mexico for unregulated healthcare services and to smuggle in medication. Children typically grow up with a single parent or grandparents even if parents are living in the same community.
What is it? 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?	
	they have arcieved confusion and fear. Given lack of resources, social trust and relatiosnhips have broken down. Decline of US incluence in global everything (political, economic, scientific, innovation, military). This leads to international power vacuum and free for all for autocrats.
What vulnerabilities does this expose?	
	Lack of values (its declaratory, not lived), communication& discussion space, aplified by shallow and superficial mass comms platforms
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
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?	slow creep of lack of everything, gradual, only relized in hindsight. At first
Question Two	**PASTE HERE**
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**
Question Two	**PASTE HERE**
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team Members:	**Grey Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	People gain their identity from their groups and we are seeing more fragmentation into smaller and smaller groups
Speaker 2	Cognitive Ease/entice people to self-reflection, and then engage with learn, and potentially embrace new truths? If you want to start a revolution, throw a better party.
Speaker 3	Meme-factories generating disinformation/What makes memes go is how well it gets absorbed. How it gets adapted. In closed societies, they are using symbols to get around censorship (rice + bunny rabbit for #metoo)
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Gen Z digital native accessing internet solely through mobile devices
Where do they live?	Dallas, TX
What is the threat?	Online meme-based Texas secession movement based on disputed 2028 federal election results and increasing divergence from "coastal" zeitgeist
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Mobile media balkanized by aggressive filter bubbling; narrow narrative frame; anti-federal government sentiment; guazy nostalgia
What is it? 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?	
	Family; social media network; all of Texas; all of the United States -- A weakened or fragmented United States -- A strong United States with strong allies
What vulnerabilities does this expose?	
	Tribalism; anti-statism; filter bubbles; balkanization; excessive fixation of self-determination
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**What is different and/or the same as previous events or instantiations of the threat?**
	Constant critique of federal disaster relief and other "local" issues;
	continued local "devolution" narratives about the preference for local solutions
	loss of prevailing federal government counter-narratives, owing to norms or regs
	computational amplicifation and A/B testing
	population completely cut off from federal support; FEMA, education, medicare/social security, texas only news stations, etc.
Question Two	**What will the person have to do to access people, services, technology and information they need?**
	Govt
	News
	New laws and norms, i.e. state constitution will become dominate (1st amendment changes?)
	exposes weak state governemnt infrastructure, what happens when social security checks, agricultural subsides, etc do not come
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**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?**
	(Federal-sponsored) counter-narratives
	Skepticism of outsiders
Question Two	**PASTE HERE**
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team Members:	**Orange Pawn**
Experience Title:	**Debbie's Dilemma**
Estimated Date:	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 Slot)	
Speaker 1	World wide this gen pays attention to what is coming out of Silicon valley and don't want to be left behind
Speaker 2	off shoring of critical infrastructure--technology talent
Speaker 3	Faux insiders
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Debbie, 31, an Asian-American journalist living in LA working for a Chinese business media company (a la Dow Jones), 2nd-gen American, English is first language, fluent in Mandarin Chinese; her professional audience is diverse business professionals, investors, etc., across Pacific Rim. Her friend social network reflects diverse American population but family is mostly of Chinese descent
Where do they live?	LA
What is the threat?	She has been asked to write a series of damaging articles (information both true, but damaging and untrue) about Amazon with the intent to influence its stock price (destroy investor confidence) so that it needs to sell to China, who will then have access to all consumer data and cloud-based web servers. Agreements Amazon has with DOD, etc., other government agencies, are now potentially available to China.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Debbie has both a moral dilemma -- she wants to keep her job, but she also surmises this is capitalism at work and this is part of how the global economy works. As a financial journalist, her narrative frame is not always an objective picture but rather is pro-business. But now, she's been asked to write something that is patently false, which is a new level of deception. Her loyalty to her job and her loyalty to country are at odds. Debbie has a revelation at this juncture that there is signficant malfeasance on the part of her employer and/or the Chinese government. She wants to investigate the extent of this but now is not sure who to trust.
What is it? 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?	
	The adversary wants to achieve technological, financial and intellectual property, as well as leverage over the US govt. The instruments of national power via information (technology, IP, consumer data) and economics.
What vulnerabilities does this expose?	
	Consolidation of cloud-based services, the ownership by corporations of massive amounts of customer data, the stability of ths US stock market; Chinese acquisition of Amazon as a result of market chaos partly induced by Debbie's articles would further exacerbate the technological off-shoring of US IP and tech know-how; and also expose the US government to massive amounts of government information/data now being controlled by Chinese government (all the government services that run through AWS, including massive amounts of US DOD data and communciations)

PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	She was assigned a series of stories by her Chinese-owned publication that contain damaging allegations about Amazon. Sources that were fed to her were vetted, but were deceiving her (company set her up to follow a certain investigative path). She has access to confidential information that her company is pressuring her to report but that compromises her journalistic ethics. But she wants to keep her job. Action that led up to event: pressure (including elements in her employment contract) to develop her personal social media network and fuse that audience with her journalism work, but without attribution.
Question Two	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	Reported information will bring down Amazon and US financial markets, China is able to buy Amazon, all its IP, all its web servers, all its customer data. No place to buy goods because physical marketplaces have been eaten by Amazon. Ripple effect into smaller ecommerce and goods manufacturing businesses. Ripple effect into transportation companies and social science research (Mechanical Turk). Government agencies and private companies reliance on Amazon cloud services. Theft of IP and patents.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**

Question Two	**PASTE HERE**
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team Members:	**Brown Chip**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	The Industrial Revolution made the US what it is but the US is no longer in that econmic state. - Institution are inadequate to address the present much less the future and will brake the paradigm.
Speaker 2	privacy is changing - used to be that there was a specific difference between private informatioin and public information; public spaces and private spaces; separation between public/work, public and social, private and social, private/family, etc; --now those borders have eroded both by virtue of the intrusion of media/social media, and by reconceptualizations (and exploitations) of what is personal/private/public - comes with risk - we need greater awareness of the changing nature of privacy; how do you develop empathy online with only screen-based cues?
Speaker 3	amplification/manipulation
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Jaunita Doe - Hispanic heritage, 28yoa, catholic, 1st generation college, single but living with a male partner, immediate and extended family living throughout Southwest US,
Where do they live?	Denver, CO - genetrified downtown area
What is the threat?	Serious (Sorting) peaceful movement to seperate Red/Blue in the United States
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Ms. Doe is of the blue pursuassion and fears no mobility in a Red company but living in a Blue neighborhood. The uncertainity of what is happening, not knowing what to do. 2nd effect of loss of federal funding to local services Ms. Doe. 3d effect is loss of confidence in ecomomic drivers.
What is it? 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?	
	Ballot propositions i.e. this state will join Blue America or Red America
What vulnerabilities does this expose?	
	The extreme polarization of the United States
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**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)**
	Delivery is the same because of the peaceful nature of the transition
Question Two	**What is different and/or the same as previous events or instantiations of the threat?**
	Dissolution of the Soviet Union
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**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?**
	An appeal to the allegiance of the military. The federal military allegiance does not allow for fracturing.
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?**
	The state governments must engage in collective action to resist federal coercion not to sucede.
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	

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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team Members:	**Black Pawn**
Experience Title:	**The New Lost Generation: Bracing for an Infinate Gap Year**
Estimated Date:	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 Slot)	
Speaker 1	Children that grow up watching their parents spreading weaponized memes will think there's nothing wrong with having political leaders who behave that way and in fact may prefer it
Speaker 2	things are subtle:memes, not quoting sources, complexity of language, signals&signaling, rhyming as away of signaling meme, playground bullying with machine learning, signals get the confirmation bias going
Speaker 3	Faux insiders
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Penelope is a teenage girl is finishing high school who is coming of age in a time when there are no certainties of "truth," and there's no "off." She's been swayed her whole life by narratives that are informed by half or false narratives. She's never really developed her own point of view, spending more time reacting to input rather than shaping it herself with original thought. She's looking at what's next for her path once she's completed high school.
Where do they live?	San Francisco
What is the threat?	Her sense of truth has no boundaries, no guidance, no foundation. She has lived most of her life responding to memes, stories, narratives that were fed to her, without guidance and practice on how to analyze, interpret, and internalize what it means to her. Most of her education has been through user-generated, online, real time content. Throughout her life, she's experienced the continued development of deep fakes influencing major societal outcomes. Facts blend with fiction, and she can't tell the difference.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Given that Penny has had so little practice developing her own voice and argument, she suffers from depression and massive self esteem issues. She's lacked role models who demonstrate a measured and thoughtful approach to engaging wtih the world. As she prepares for adulthood - for launching from her family's care - she's rutterless. In desparation, she "forces" causes on herself for direction, but snaps back into depression when she can't find authentic connection. She's disconnected. She's lonely. She needs a hug.
What is it? 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?	
	She's watched her parents - particularly her mother - get distracted and dismayed by technology and the state of civil discource in our country. After the 2020 election, her mother became preoccupied by the conspiracy theories and media hijacking by anger and tribalism. Throughour her childhood, she didn't have present parents to guide her and help her understand the context of her world, and her role in shaping it.
What vulnerabilities does this expose?	
	Manipulation is age and demongraphic agnostic. Isolation can occur even in well intended families and that social media forces - particularly backed by negative intent are very powerful isolating forces that can lead to a feeling of helplessness and lack of place in the world.

PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	What is different and/or the same as previous events or instantiations of the threat?
	It's amplified, it's omnipresent in every facet of her life, it's inescapable. This is the new "normal." At every table in every restaurant, they are tapping on to their neural network chip that takes them to alternative realities, fueled by bots and memes. The early trends of isolation and depression have gotten to an extreme. No one knows how to have a real conversation - face to face - anymore.
Question Two	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	This isn't just Penelope. There are millions of Penelope's out there. What are they passionate about? Where are they going to work? What is going to motivate them? How might their social development get stunted? What are the implications for the next generation?
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**Business Models: What new business models and practices will be in place to enable the threat? How is it funded?**
	Silicon Valley extreme, now fueled by even more types of funding mechanisms - instantaneous crypto-currencies in exchange for time spent online or in the cloud.
Question Two	**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?**
	The tech companies are already doing this - they are creating addition devices, fueled by addictive "drug-like" experiences. This is very little regulation or self-policing of the development of these potentionaly destructive devices. The government is woefully behind in understanding the true nature of this emerging threat, and in many ways, complicit in furthering the threat. Scientific studies take too long to come back with conclusive guidance and evidence on the impact of this relentless input on the developing brain.

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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	Parents and families (informed and engaged)
2	School systems
3	Peer groups, community engagement/organization/spiritual engagement
4	Government - standards
5	Industry find a conscience (self policing)
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
1	Accessibility of devices and ubiliquity of (false) information
2	Opaque algorthims that drive continuous feed of information
3	Alarm mental health behaviors - rise in obesity, markers of poor self care
4	Lack of matriculation to college/ College drop outs - the "infinite gap year"
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?	
1	More awareness of negative impacts of social media and weaponized narratives to teens - "This is your brain on social media"
2	More proactive self-regulation by companies, inspired by their new chief "ethical" officer
3	School mandates more person-person engagement (the new "PE")
4	Curriculum developed to support self-discovery and personal values, and individual agency
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?	
1	Adopt google's 20% time allocated to no-tech
2	Government shuts down networks one night/week to mandate quality time
3	Rewards/stipends for joining commuity organizations
4	Campaign finance reform - public funding for elections. Period.
5	

Team Members:	**White Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Very committed to causes, more serious, understand hard work
Speaker 2	off shoring of critical infrastructure--technology talent
Speaker 3	meme is something that spreads like a disease vector; what's new is memes that cause action in the real world.
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Xi Jinping
Where do they live?	China
What is the threat?	The Authenticity Revolution against the ancient regime that seemed so triumphalist in 2019.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Every TTP that they've developed to maintain power is collapsing around them. Colonial backlash in Africa and maybe Southeast Asia. Rich and young are leaving. AI's are going all wrong because the data it was learning from was all based on human behavior that turned out to be all wrong. Backlash against workism, complete with 12 step programs. The demographic catastrophe of being the first country to become old before it became rich. Very few Generation Z'ers. The intent, coordination, and influence of chinese citizens to covertly signal counter narratives dramatically outpaces the top down cencorship of the regime. A black market emerges in manufacturing hubs to rapidly produce countersurveillance products. Trojan horses are planted by their adversaries to use their own tactics against them. The Uyghur population is prevailing against the odds -- because they are authentic.
What is it? 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?	
	The Authenticity Revolution. "Never trust a reality you can't touch." "Never trust a 'reality' that is multiplatform and multimedia." "I don't want to live in these fake cities." "Fake food." It's the calling bullshit revolution. A return to spirituality. (Confucianism nostalgia?) Status symbol: Shinola watches.
What vulnerabilities does this expose?	
	Demographics. Erosion of "the veil" of social control. Social credit system -- how many sheets of toilet paper are you using.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	Xi Mingze (simplified Chinese: 习明泽; traditional Chinese: 習明澤; pinyin: Xí Míngzé; [ɕǐ mǐŋ.tsɤ̌]; born 25 June 1992), nicknamed Xiao Muzi (小木子, lit. 'Little Wood'),[1] is the only child of Chinese paramount leader (CPC General Secretary) Xi Jinping[2] and folk singer Peng Liyuan.[3]
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	**PASTE HERE**
	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	Xi Mingze -- Xi Xinping's daughter, Handmade in China, Artisanal movement in China, Fake news/cities/jobs/communism/lives, "I'm taking the stairs" as an act of resistance, propaganda that you can believe in
Question Two	**PASTE HERE**
	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)	
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?	
Question One	**PASTE HERE**
	Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?
Question Two	**PASTE HERE**
	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?	
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?	
1	
2	
3	
4	
5	

Team	**Blue Pawn**	
Experience Title:		https://ssi.armywarcollege.edu/pubs/parameters/articles/2010winter/Dunlap_Jr.pdf
Estimated Date:	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 Slot)		
		Fake Doctor Farm
Speaker 1	Children born after mid-90s are most diverse in terms of friend circles and preferences. Both societal values and because of the digital tools available	
Speaker 2	off shoring of critical infrastructure--technology talent	
Speaker 3	Funded Coopted Media	
PART ONE: Who is your Person?		
NOTE: Remember to give as much detail as possible. The power is in the details. Scribes please write as though you are writing for someone who is not in the room.	**Age 29, Female, CDC communications**	
Who is your person and what is their broader community?		
Where do they live?	Digital World	
What is the threat?	Erosion of narrative of western liberal democracy, regulatory failure, industries based on trust fail (example - medical) predicated by weaponization of narratives, weaken society, make less resilient --> Shock -- pandemic --> nation states fail	
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.		
	The Event: A catastrophic global pandemic is experienced worldwide placing a severe need on medical workers. Ten years of narrative campaigns has deteriorated trust in the health care system leads to ineffective treatment of the disease.	
What is it? 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?		
	lack of trust rust in government for Ebola crisis, lack of trust of health care companies & phrameceutical companies	
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)		
Questions (pick two)		
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?		
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	**PASTE HERE**
	The Event: A catastrophic global pandemic is experienced worldwide placing a severe need on medical workers.
Question Two	**PASTE HERE**
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**
Question Two	**PASTE HERE**
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.	
Gates:	
What are the Gates?	
List out what the Defenders (government, law enforcement, industry, etc) 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	
Flags:	
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.	
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?		
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?		
1		
2		
3		
4		
5		

	Red Pawn
Experience Title:	**US Education: Made in China**
Estimated Date:	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 Slot)	
Speaker 1	Participatory parenting
Speaker 2	Attention Economy
Speaker 3	"Weaponized paranoia" is a real threat
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Eighteen year old US citizen about to vote for the first time
Where do they live?	US
What is the threat?	There is a financial crisis in the 2020's /recession. China comes in and buys many US businesses. Government's cut funding for education and move to more online education models to save money. China has aquired texbook manufactures and online education platforms and is using them to deliver customized education experiences that have subtle AI-enabled, personalized, information manipulation tools that promote pro Chinese positions and anti-USG positions. These are all subtly different from student to student, so it is very hard to put together the full picture of the manipulation
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	They have been in the curriculum for the last 10 years and are now anti-USG and very pro China
What is it? 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?	
	Their peers, family, community and country are involved. China wants a generation to have pro-China views and anti-USG views so they can take coercive military and economic action in E Asia and Africa. China wants Generation Z to think its not essential to live in a democracy; that the Chinese model is superior China is afraid of a unified US challenging their hegemony. China is afraid of US keeping them out of their education market. China is afraid of being exposed as manipulating the public. China wants their international image to be positive; is afraid of being seen as manipulative/evil They want the US divided and focused on internal sqabbles; they want democracies divided
What vulnerabilities does this expose?	
	Theyve been brainwashed; hard to change their mind
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	China takes military action in E Asia. Josie is voting in an election where one candidate is
Question Two	What are the broader implications of a threat like this? What might a ripple effect look like?
	Ripple effect is that its almost impossible to get Generation Z to change their belief. No longer support for promoting democratic values worldwide. Tolerance of authoritarianism.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?**
	Buy texbook companies and online education companies. Fight off laws or regulations against these kinds of acquisitions "free market", "no government regulations". Need psychometric profiling data on the students (easy with htird party transfers of data); need market share - reasonably effective product; state subsidies to undermine competitors
Question Two	**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?**
	Advances in customized online education; AI tools focused on education, manipulation and persuasion; data hacks
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.	
Gates:	
What are the Gates?	

List out what the Defenders (government, law enforcement, industry, etc) 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 could limit the types of businesses/industries allow nation states
	2	An AI auditing system that monitors for systemic manipulation a
	3	Education courses about the information environment, scientific critical thinking, online manipulation
	4	Nationalize the education system. Go back to centralized, approv
	5	National service programs to build national unity and unified narr
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		
	1	Serious economic crisis that leaves the US vulnerable
	2	Significant advances in AI manipulation technologies
	3	Potential Chinese domination of the technology ecosystem and r
	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?		
	1	Mandate programs/tools for identifying coordinated manipulativ platforms
	2	Implement critical thinking educational program
	3	Have broader government review of foreign purchases of US cor company access to US citizen data
	4	Congrssional commission on data privacy, information security, generate recommendations
	5	Parents must actively participate in curriculums to monitor for m
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?		
	1	Pass legislation?
	2	Implement a national civics course to all students that is develop multistakeholder group

FUTURES WORKBOOK DAY TWO

Team Members:	**Black Chip**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Marketing and product-oriented organizations control the technology Limiting or controlling the tech is not viable; too many interests; dual-use with positive/negative uses; whole of society contexts make it useful for many different domains
Speaker 2	Who is the arbiter of veracity? Democratic action requires an informed citizenry, so accurate information is a public good, but at the same time free speech is a cherished, national-identity-forming value, which puts into tension establishing an entity for vetting information accuracy vs. stifling free speech; "Provide some easily digestible information provenance to help people verify information. People have to care that they are being gamed, before they can begin to fight the problem. Some people are blissfully ignorant; some people have bigger problems than to care about the existential threat of misinformation. People think ""the media"" are at fault. Truth is socially constructed, so it is not unconditional. Where is the common value?"
Speaker 3	Funded, coopted media; Funded, coopted medianarratives reinforced / transferred into the mainstream / enhanced credibility
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Pete is a retired military officer, who spent six years on different deployments overseas. This work tempo left him divorced and his 2 adult kids are somewhat strangers. Pete retired in 2028 and quickly went to work for Wikipedia, 6 months before Wikipedia went bankrupt, so he began teaching at a public high school. Then the public education system was defunded because of lack of interest. Pete is now out of a job and finds himself unemployable.
Where do they live?	Phoenix

What is the threat?	Helicopter parents choose certain AI tutoring systems that can shape their childrens' identities to fit a particular tribal norm, world view, or pathway to success. Some of these AI tutoring systems have been co-opted by the "wings" of politics (alt-right, alt-left, theological, etc) and are creating very distinct tribes who will not see eye to eye. Truth becomes only as wide as the tribe and the constructed identity allows. Pete becomes unemployable because he has an obsolete vision of what education is and his online identity (which is the only one that now matters) does not have the "credentials" to belong to a tribe. He is the "universal other".
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Intelligent tutoring systems are sophisticated enough to provide students a individualized curriculum that feeds and supports whatever tribal narrative is desired (by the student, the parent, peers, etc). Pete is again out of work.
What is it? 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?	
	The "adversary" is the constant pressure from other tribes who are trying to "capture" the identities of impressionable children from other tribes. Constant war of all-against-all with the goal of shaping children's identities.
What vulnerabilities does this expose?	
	Identity is no longer spontaneous but is defined by tribe as a defense mechanism against the "other." Real-world actions are highly influenced by online identity.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**What are the broader implications of a threat like this? What might a ripple effect look like?**
	Not only can Pete not get a job, he is ostracized by his family and some of his former friends because he refuses to be part of a specific tribe.

Question Two	**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?**
	Pete begins to hear about proposals to defund public education through news media, but when the decision to actually cut funds occurs, he is at work teaching a significantly reduced classroom size, and the principal comes in and says, “go home, your job is no longer available. The school is shutting down effective tomorrow.”
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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 develope	
Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Acto	
Question One	**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?**
	Development and widespread use of individualized AI tutoring systems. The more popular ones (i.e. “cheaper” and more accessible) are available because of funding from alt-wing groups who insist on their version of truth being the training models for that version of AI. “Tribal” groups are funding their own curricula that is tailored to a singular point of view and is as appealing as possible. Behavioral economics, neuroscience, personal psychology, and marketing principles are strongly emphasized in order to spread particular product lines.
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?**
	Laws, cultural norms, and employment are changed to enable tribal based education/indoctrination. There is a culmination of years-long attack on the concept of public education.
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.	
Gates:	
What are the Gates?	

List out what the Defenders (government, law enforcement, industry, etc) 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.	Military, intelligence, security organizations; maybe corporations	**WHO?**
1	Safe AI development principles (transparency, bias, privacy by design, etc)	
2	Trying to protect education as a public good with society wide standards - the right to fight is important here, not the curricula or outcomes	
3	Appointees to Supreme Court that act against polarizing tribal influencers	
4		
5		
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Public perception of the federal government.	
2	Definitions of "truth" are no longer in the wheelhouse of science. Trust in traditional knowledge development organizations fails.	
3	Failure of Wikipedia	
4	"Chip in the brain" tech allows instant flow of video/media/emotive content, but heavy content filters are required so people don't go insane; these filters are designed by one's AI tutor	
5	Public education as a private good at a much larger scale than in 2019	
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?		**WHO?**

1	Rise of at least two additional strong political parties	
2	Strong adoption of safe AI principles by industry leaders; maybe by government	
3	Discussions of AI conversations on effects of education	
4	Mandatory military draft provides requirement for people to come together for a unifying purpose	
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?		**WHO?**
1	Viable third party strong presence within government	
2	Discourse of disagreement is acceptable again	
3	Financial safety net for public school funding	
4	Part of Pete's military transition is prepping him for tribal membership	
5		

Team Members:	**Green Pawn**
Experience Title:	**Seeds of Doubt**
Estimated Date:	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 Slot)	
Speaker 1	??????
Speaker 2	?????????????
Speaker 3	!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Lily Smythe, farmer and single mother, (eventually) local and internet celebrity. Secondary: Thomas, the 13-year-old, extremely tech savvy child who helps run her social media presence.
Where do they live?	Small town Iowa where local industry is primarily soy farming.
What is the threat?	Lily's status in the community makes her a high-value target for multiple entities. Local energy and water firms are trying to buy her and George's farm for the land, as is multinational lobby SoyCo - which already has interest in most of the farms in the area, and whom Lily has spoken out against in the past. A corrupt group within an existing political party wants to gain voters, and has identified the mother, Lily, as a possible 'swing person', where if she were to openly and expressly support their presidential primary candidate they would win the seat.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	1st: George seemingly abruptly leaves Lily for Carol, a younger community member who is also the daughter of SoyCo's U.S. representative. 2nd: Lily's farm, Smythe Soy, loses some (but not all) intellectual property via George abdicating with it and giving it to Carol, who, it becomes apparent to Lily, is an agent of SoyCo/PRC. 3rd: Tom (Lily & George's 13 year old son), is the subject of vicious cyber attacks, troll farming directed at 'befriending' Tom and directing him toward certain coping mechagnisms (as he is desperate for positive reinforcement amongst his peers), which has cultivated addiction through augmented reality to first online gaming and later porn. He is ostracized from his friends group at school and falls into a deep depression. Meanwhile, Lily is subjected to unbenownst to her, a personalized social engineering-based propoganda campaign pushing her to endorce the Soy Lobby's Presidential Primary Candidate.
What is it? 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?	
	Multiple adversaries from all sides - Pickens Holding (wants the land), SoyCo (wants the land and to kill the Intellectual Property, and to silence Lily's advocating against them), PRC (major funder of SoyCo, wants to obtain the I.P. for use on a global scale, dominate U.S. Soy Industry), Soy Lobby & Presidential Candidate (want to obtain Lily's vote and endorsement in order to swing Iowa.
What vulnerabilities does this expose?	
	Lack of physical and digital security on behalf of Smythe Soy, lack of operational awareness on behalf of George (getting honey potted), Lily (whose reputation is destoryed), and Tom (whose mental health declines as a result of targeted attacks and subsequent addictive behaviors / maladaptive coping mechanisms).
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	

Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	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?
	1st: Lily sees her husband's infidelity and abandonment of their child as a betrayal, and does not initially connect the dots to the larger economic scenario playing out. Tom feels victimized and attacked, and sees no outlet except the maladaptive behaviors (porn) he adopts. Neither initially see the bigger picture, that all of this has been orchestrated by SoyCo via PRC to obtain intellectual property, discredit Lily, and - when she is on the upswing of recovery from the attack - use her newfound celebrity status to garner votes for the Soy Lobby (also funded by SoyCo's) chosen presidential primary candidate. Neither will pick up on the social engineering aspect of the campaign until later, when Tom and his tech savvy friends discover that his addictions and Lily's discrediting are the result of personally targeted initiatives derived from pattern of life analysis of the two and unwitting input from George to Carol.
Question Two	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	Social engineering and personalized propoganda campaigns will be much easier and cheaper to accomplish, and will likely happen on a much larger scale in the next ten years. They will have the opportunity, as well, to bleed into the real world through the internet of the things (will you like a political candidate more, if you listen to an advertisement for them while driving to work on a day where you hit no red lights?).
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**
	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?
	Social Engineering, Augmented Reality, Disinformation Campaigns. Adversaries will be able to easily take advantage of a person's interconnectedness to their online presence, career, business, and personal life, to systematically destroy/disrupt/interrupt access to all of it through targeted attacks at another vector (attacks on personal life can more directly effect career, etc.)
Question Two	**PASTE HERE**
	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?

	Social media presence tied into everything, augmented reality/videogames and at home entertainment systems, "hyper-responsive machine learning-aided seduction" techniques (C66), internet of things; OSINT collection tools used by counter-misinformation "militias", social media bots; increasingly connected and automated agricultural techniques and technologies (automated combines, etc)	Carol able to create cognitive composite from George's psychological tendencies gained from Church's database, bought from black market, programs AI with goal of helping her seduce George (both in-person and distance attacks) - prompts her conversation points, introduces newsletter/magazine choices - ubiquitous all-platforms influence operations
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.		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Observation of online troll farms, AIs, and other elements typically responsible for disinformation and propoganda campaigns.	Watchdog groups
2	Laws and regulations concerning campaign tactics.	U.S. Government
3	Privacy laws - creates loopholes and pushes corps to extremes to avoid violative activity	U.S. Government, Corporations
4	Intellectual property and patent laws, protections, and enforcement / system for punishing violation.	U.S. Government, local law enforcement.
5	Nurtured distinction between a person's 'real' self and online persona, particularly when it comes to persc	Community members, friends, family.
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	'Omnipresent' advertising / life experiences (if it feels directly targeted to you, it probably is)	Cambridge Analytica style advertizing firms
2	Self-directing AI/bots	Large corps, states
3	Ubiquity of AR systems and evidence of addiction	individuals
4	Foreign governments purchasing American farmland	States, corps
5	Tangible and data selves, businesses no longer separated - IoT	individuals
6	long-distance commercial drones	corps
7	production of synthetic, biodesigned pathogen capable of targeting individual crops/species	corps, individuals
8	increased vulnerability of important American industries (importance of novel production techniques will increase as population expands) and infrastructure to intellectual property theft	corps, small businesses, small business owners.
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?		**WHO?**
1	Pass a nationwide, federally enforcable ban on subliminal and covert social engineering campaign tactics.	U.S. Government
2	Creation, enforcement of anti-interference/anti-intevention/anti-corruption acts to protect American citizens from, specifically, social media and reputational attacks with malign intent	U.S. Government/European Union
3	Actionable ban on the targeting / online manipulation of underage persons. Treaty?	Regulatory agencies, NGOs, governments.
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?		**WHO?**
1	Increased societal awareness of the threats technology may pose to one's psychology, etc., awareness campaigns or 'common knowledge' adopted to combat malicious online reputation attacks.	End users / citizens
2	Increased interest in, understanding of, and use of internet security programs and tactics.	End users / citizens
3	Increased attention to the affects, abilities, users of augmented reality systems	End users / citizens / governments
4	Awareness of intentions of foreign government-owned corporations - goals/plots to purchase American companies to affect value of exports to fulfill both foreign policy and corporate goals	Individuals / citizens
5	Global buy-in from individuals operating in the globalized field - people need to learn to care, on a regular, natural basis, about more than their small local communities - as interconnected actions gain broader overall effect	Individuals / citizens
Overnight Thoughts:	Though there will be more technological opportunities for threat actors in 2029, there will also be more opportunities for would-be victims to defend themselves and take action. Once Lily discovers that the attack against her personhood was a malicious act of economic espionage designed to destroy her life. Technology enables people to 'punch above their weight', which will likely grow in the next ten years. In 2029, it may literally be something as small as the town's local 4H club seeing the attack as more than just infidelity, reaching out to her, and initiating a counter-disinformation campaign against the corporation's (on behalf of a foreign state's) actions to slander and discredit Lily.	

Team Members:	**White Chip**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Enjoy reflections by friends on things they already like and using tailored tools: not on same tools as the other generations. Utube Channels and peers networks
Speaker 2	privacy is changing: used to be that there was a specific difference between private informatioin and public information; public spaces and private spaces; separation between public/work, public and social, private and social, private/family, etc; --now those borders have eroded both by virtue of the intrusion of media/social media, and by reconceptualizations (and exploitations) of what is personal/private/public
Speaker 3	Rise of deep fakes
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Bubba, the CEO of a AI and Quantum Computing Company, on the brink of a breakthrough in quantum computing.
Where do they live?	Bubba lives in high tech center of the United States, North Dakota. His conservative stance and leadership at his company have positioned it at the forefront of the industry, and is seen as a visionary leader that can see opportunitys that others miss.
What is the threat?	While negoting with a tech company in Paris to leverage their collective S&T investment, a Deep Fake (real time teleconference manipulation) is empoyed by Finland to order a shift in partnership to move all the quantaum communication intellectual poperty a competitor in Finland.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Bubba has seen within his social networks and peer networks that there are several companies on the brink of matching their tech and IP in secure quantum communications. Pressure from investers to make a deal exploit their technological advancement before being overtaken. A problem is that they really is not competitor. A team in Finland (an EU but non NATO nation) has inflitrated his peer trusted network and their misinfirmation campaign has convinced both his company and investors that several world wide competitors will beat them to market. The French Firm (EU and NATO) appears to have the most compatible technologies and he is looking to partner and execute quickly to solidify market position. European privacy law and differing ethical and export restrictions make securing a European partner possibly exstremely lucrative, but there really is not advantage to partnering if they have a unique technogical advantage.
What is it? 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?	
	The company, investors and community in North Dakota that have grown up to support this new tech hub and emerging technolgies. Mainstream public is concerned about the privacy and possible national security implicaitons of a deal.
What vulnerabilities does this expose?	

	Security of communication, inadequete and obselete regulatory framework. Intellectual propery laws and legal framework are obselete and cannot keep up with modern business cycle and tech driven deals. Vunerability to semi-closed peer networks that have high trust but can have misinformation campaign within the echo chamber that is biased towards action.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?**
	Bubba, while lunching with the Parisians to celebrate the deal, his phone alerts him to traffic within his trusted peer networks communitions platform that the deal is complete and merger with the Finnish company is company. He jokily responds to his trusted company mates and investors in the trusted channel, you are very funny, we all know the deal en Francais. The trusted channel blows up as the investors question waht really is going on. Seeded information outside of their trusted network starts to report privacy activists organizing against the company due to the new merger with the non-NATO parter of the Finns.
Question Two	**What are the broader implications of a threat like this? What might a ripple effect look like?**
	Transfer of critical IP threating nattional security and privacy issues. Economic distruption in the North Dakota Tech hub. Lack of investor confidence in "unicorns" and quickly growing tech firms creates a disruption in the economy. The lack of security now risks confidence across defense and national policy apparatus as well. Threat of government intervention as the company has violated export controls and regulatory requirements.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	

Question One	**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?**	
	Finnish company trying to work around the restriction to export control outside of NATO. They don't currenlty have the technology to exploit or market the secure communitions thoughtout the EU, but this merger would allow them to quickly position as the leader within EU, and support ANTI-NATO bias on the continent. They need the technology to create a real-time deepfake attack on video teleconfence in a peer to peer believed secure communication network. EU privacy and legal frameworks and law enforcement will be overcome by quickly tranfering the IP to their networks within the sorveign borders of Finland. Using privacy tools mitigate against disclosure, but also having positioned the narrative that the company had individually developed similiar technologies and was positioned as potential EU leader.	
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?**	
	Need members of trusted networks that are witting or unwittily supporting the deepfake messaging. Press support of the released and manipulated disinformation. Criminal elements assist with planned and identifying witting participates in the sceme. Government support once IP has been stolen to back up the claims of the IP being developed within the EU. Narrative support to delay any regulatory or legislative action until after the transfer has occured.	
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.		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Regulatory and Regulatory controls to allow verification at speed	Government
2	Legislative, investigatory, and regulating process to protect and verity IP in new realities	Government/Industry
3	Self policying / Voluntery Industry control on tech transfer	Industry
4	Government/Industry sharing of more robust secure communication networks	government/industry
5	Cybersecurity to identity source of information as well as communication means	government
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Ability to insert deep fakes in real time into video communications	
2	Market develops for telephone spoofing and anti-spoofing technologies	
3	Develop of soverign internets that provide extensive protection once IP leaves US	
4	Inteligence community signals with regard to industrial espionage	
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?		**WHO?**
1	Trustable intellegience sources that are vetted and provide actionable tips	USG
2	New regulation methods early in tech process that allows to share, license and partner in a way that would take away the incentive/economic benefit to steal IP	
3	Education program for populations to understand the limits of security with regard to communications	
4	Needs procedures to address and mitigate for stolen IP	
5	Develop central clearing house of secure communications technologies	
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?		**WHO?**
1	Employ quatuum communications technology at scale to allow for quantum entenglement to create 100% communications medium.	
2	Education on the limits of AI and deepfakes technologies and detection limitations	
3		
4		
5		

Team Members:	**Black Pawn**
Experience Title:	**The Decline of Higher Ed and Rise of the Anti-University: Hyper-individual, individuated, decentralized higher ed**
Estimated Date:	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 Slot)	
Speaker 1	Protests challenging DoD working with corporate America. The generation should influence what projects their companies undertake not just what individual projects "they" undertake.
Speaker 2	Tunnel vision, desperation in the face of change
Speaker 3	Rise of deep fakes
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	President of ASU, Michael Crow
Where do they live?	Phoenix
What is the threat?	Attracting high quality students, faculty, funding to viably support quality education that supports critical thinking and creative capability in an age of digitization of content that's ubiquitously available, for free, from credible and non-credible sources....that's available to be implanted in a student's brain.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Higher ed is under attack everywhere. Student enrollment is down considerably. Faculty salaries and benefits need to be paid, so debts are rising, limiting investment in new research and teaching. State funding is down. Faculty are being picked off by industry. Research is being taken over by private industry. Buildings are empty.
What is it? 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?	
	Board of Governors/State Board. Existing Faculty & Administrators. Current students. Alumni are frustrated about prospects of the future. Giving is down significantly. Industry are not recruiting as heavily from current student base. The biggest threat is irrelevancy, and ultimately solvency.
What vulnerabilities does this expose?	
	The biggest threat is irrelevancy, and ultimately solvency. What can you distinctly offer students, faculty, and ultimately society from a higher ed degree/experience. It also exposes students to questionable "education" - what are the quality metrics of what constitutes high value secondary education? If students go towards highly personalized education, they choose their subjects and sources. Are they verified? Are they based in in foundational knowledge? What are the standards?
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?**
	Research funding that was designated for ASU gets reallocated to private startup (Alter Ego?) and LInkedIn Learning pursuing individually delivered curriculum sourced from multiple mediums

Question Two	**What are the broader implications of a threat like this? What might a ripple effect look like?**	
	Enrollment continues to decline. General Liberal arts degrees are dwindling. Decline of Pheonix economy do to talent drain and student drain - housing, services, infrastructure, etc. Trend scaling across the country. More large insitutuions, like Ohio State, struggling to hold on to foothold and conribution to their local communities. More students are falling prey to "deep fake" degrees.	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)		
Questions (pick two)		
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?		
Question One	**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?**	
	New players are entering the higher ed business at the same time that regulation is crumbling. Anyone can offer a "higher degree" equivalent from a combination of linkedin, youtube, and direct to neural pathway. Meanwhile, companies are recruiting young talent earlier and earlier, and use external education arms to help recruit and develop that talent for the company. Soon, you can get a degree in Fortnite	
Question Two	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**	
	AlterEgo, neural implants, ubiquitous video feeds (via deep fakes), XR (AR & VR) environments create multiple pathways to higher ed.	
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.		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Accredidation boards get stricter on who can awards degrees	Academia and government
2	Financial incentives to finish traditional higher ed (tax incentives)	government
3	Universities offer new partnerships with industry	University
4	Industry creates more scholarships for traditional higher ed	Industry
5	More community support for families of students to attend and support college	Academia and government
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	LinkedIn Learning offers its first undergrad degree; Halolens offers VR equivalent	LinkedIn Learning
2	Fortnite partners with MIT to offer virtual degree online in Fortnite	Industry
3	More companies recruiting right from highschool - google announces all time high engineering recruitment from STEM schools	Industry
4	High school college counselors start to advocate for alternative paths (vs traditional college)	Education
5	College enrollment down from prospective students	Students
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?		**WHO?**
1	Student loan crisis - affordable access to higher education	Government
2	Universities teach curricula/pedagogy that focuses on critical thinking and lifelong learning	Academia

3	Watch and research enrollment and metriculation trends carefully - connect that with long term contributions of students to society	
4	More partnerships between industry and higher ed - new curricula and hiring pathways	Academia/industry
5	Monitor incentive structure (new tax and financial benefits) and support systems to get and keep kids in college	
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?		**WHO?**
1	Better tech to identify and mitigate deep fake videos	Govt, industry
2	Revamp the Dept of Ed - to more focused on student experience. Create blockchain accreditation for its classes to demonstrate unique learning experience	Govt, industry
3	Revised immigration to allow for world's best faculty and students to teach and do research at higher ed	Academia
4	Industries continue to hire from traditional higher ed - evidence exists that higher ed has better long term employment rate	Industry, Dept of Labor
5	Academia gets rid of tenure track to release funds to be focused on students	Academia

Team Members:	**Purple Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Older generation alienated: Lack of “adult” mentorship; use of “adult” organizations to communicate to next generation (builds “tribal” societies); victory of Rosseau over Voltaire
Speaker 2	Censorship: Balance of freedom of speech and control
Speaker 3	Immediate amplication through toxic ecochambers (use to amplify disinformation); More you let it go, the dangerous it becomes
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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, white, male. Works from home as an automated robotics engineer. Lives in a single, non-binary community, and alienated from family ties. He has robotic sister wives.
Where do they live?	Coastal suburb
What is the threat?	With instantaneous autiomation and super-fast connectivity, in 10 years, 5G, automated responses and autonomous decisionmaking means that a person becomes isolated, in a bubble (Matrix style, or Descartes's brain in a jar seeing Platyo's shadown in a cave). There is no reliancde on outside human contact or interqction, as the bubble provides more intantaneous and plesant feedback. Threat: man-in-the-middle, lack of integrity, preference for a robotic instant granparent insted of the intergenerational and interhuman links.
	The complete break down of human to human communication.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Job becomes automated. He becomes completely isolated from human contact, because trust in electronic communication has become almost completely automated. Communication automation has destroyed his validation system from online likes and comments. Relies on the robtic sister wives that he programed to meet human needs (i.e. self-worth, emotional interaction). Instead of creating, discovering innovating and thus driving economy, they're in a bubble of their own making. However, all of this is controlled by extrernal servers that run autinomous decidsions (AI) with little considerastion for security of connections. Therefore, a man-in-the middle can easily take over running this life withjout detection, causing a meltdown with no social support structure to catch it.
What is it? 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?	
	Isolation of more individuals, which leads to further breakdown of society. Lack of civic participation. The Adversary is afraid that this will lead to a revolution of interpersonal communication and a strengthening of social ties.
What vulnerabilities does this expose?	
	Exposes the mental, emotional, and physical health of an entire generation. Weakness of infrastucture and over confidence of the security of the infrastructure. The vulnerability of online validation systems.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	

Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**What will the person have to do to access people, services, technology and information they need?**
	Barriers: 1. lack of skills of human interaction; 2. lack of a culture of proactive sociual services in the US; 3. lack of family or other support structure; 4. lack of available services and funding: 5. AI/ML will not help as they're not optimised for compassion but reproduction of the existing structures.
Question Two	**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)**
	Information will be constantly delivered, but none of this information will be able to satisfy his human needs or provide him the skills and wisdom he needs to survive. The only communication with others that he will have is with his robotic sister wives because he has alienated himself from family and does not trust electronic communication.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	Barriers: 1. lack of skills of human interaction; 2. lack of a culture of proactive sociual services in the US; 3. lack of family or other support structure; 4. lack of available services and funding: 5. AI/ML will not help as they're not optimised for compassion but reproduction of the existing structures.
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?	Automated communication and 'fake friends'. Influence those on social media to spend more time interacting with fake friends and then have the subject realize that he has distanced himself from his 'real friends'. This takes an emotional toll. Causing the alienation of social groups and minorities by soreading weaponized narratives about them.
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?	
Question One	**PASTE HERE**
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?	Barriers: 1. lack of skills of human interaction; 2. lack of a culture of proactive sociual services in the US; 3. lack of family or other support structure; 4. lack of available services and funding: 5. AI/ML will not help as they're not optimised for compassion but reproduction of the existing structures.
Question Two	**PASTE HERE**
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?	Automated communication and 'fake friends' as well as outsourcing of decisionmaking to external automaed systems (first, your termostat is autonomous and controlled by external server, then the algorhytms restocks your fridge; then the bahaviour of the robot viwes. Then the adversary seizes control). Influence those on social media to spend more time interacting with fake friends and then have the subject realize that he has distanced himself from his 'real friends'. This takes an emotional toll. Causing the alienation of social groups and minorities by soreading weaponized narratives about them.

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.		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.	Connectivity (Government/Google); interpersonal communication (Family (older generation)); Interpersor	**WHO?**
1	Community: not bowling alone, create mechanisms of social cohesion that replace the family ties (clubs, associstions) and thus provide identity as well as a social network; solidarity, support (a person to drive you home from the doctors when you're too sick to do so)	Americans, always forming associations; government
2	Proactive and personal social setvices, personalized appraoch in social work	Government
3	regulation on human-like robotics	government
4	ethics and research	academia
5	security of connections, security by design of services and goods	pricate sector developers, government in regulation (particularly in terms of critical information infrastructure)
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Only communities that the majority of Americans belong to are digital.	Americans
2	Companies increasingly rely on automated communication it place of human to human communitication.	Corporations
3	Widespread use of unregulated human-like robots that temporarily fill the void of human contact.	Government
4	Foreign entity presence on social media platforms that goes unregulated, deterred, or defended against.	Government
5	Polling: americans reportting having social ties, responses to quesitons about club membership	
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?		**WHO?**
1	Prepare people through public and private campaign to slowly decrease dependence on technology.	Government and private industry
2	Initiate and fund social groups that promote human interaction.	Government and industry
3	greater security on social media platforms.	Government
4	Shift from data driven to data value. Data only characterizes to a certain point. Be human focused	Private
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?		WHO?
1	Prepare people through public and private campaign to slowly decrease dependence on technology.	Government and private industry
2	Technology to backtrack all of social media friends to help verify that social media friends are not AI.	Social media companies
3	Education about tech dependence.	
4		
5		

Team Members:	**White Pawn**
Experience Title:	**The War on Authenticity**
Estimated Date:	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 Slot)	
Speaker 1	Self organization takes place now in cyberspace because of the limits of the terrestrial space.
Speaker 2	off shoring of critical infrastructure--pharmaceutical, manufacture
Speaker 3	New ways to sift through analysis of information (AI programs, more off the shelf options)
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Zhang Dayi -- Leading influencer in the Wanghong economy
Where do they live?	Dashanzi is the art district of Beijing
What is the threat?	She's at beachhead of the War on Authenticity
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Zhang logs on Monday and realizes that "logging off" has become a meme of authenticity that has spread virally. Subsequently she receives a hand delivered letter by one man in a black suit where she is summoned to meet with the Minister of Wanghong.
What is it? 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?	
	Zhang didn't mean to become a symbol that would launch a revolution, she just wanted some for her secret life, but what she didn't realize is that she set off a red alert in the regime that triggered her team, handlers, and representatives to urgently contact her while she's off the reservation. She has cut off her data for the weekend. “All human beings have three lives: public, private, and secret.” — Gabriel García Márquez,
What vulnerabilities does this expose?	
	The achilles heal is the granularity of data they've become dependent up to feed their AI which is the foundation of their social control and their economy. The Chinese regime has woken up to how vulnerable they are to the inevitable cussedness of humans. Who are *never* machines.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	When Zhang receives a hand delivered physical letter, she realizes the signifigance of her actions. In a synthetic world, receiving something material from someone phyically appearing on her door step signals just how far out of line she's gone. She has been put on official notice. Her account has been frozen and her publishing key's have been removed. She has no ability to post or contact with people. The littany of the fake that people have to come to quietly abhor: fake reports on natural disasters, fake government reports about official corruption, fake government reports about disease, fake government reports about prosperity, fake government reports about crackdown on muslims, fake veil of safety and security, fake reports about potential adversaries, fake government reports about the success of Chinese colonialism, fake impression that people are happy, and fake genese are being added to their children. Very little of the experienced reality matches what is being pushed and seen to them online. The events and symbols that were acts of resistance that led up to the Authenticity Revolution: young people made the quiet action of taking the stairs instead of the elevator, people decide to take the scenic route to work instead of the most efficient path, people choose to not to put biometric sensors, a fashion movement towards anti surveillance apparel emerges, black market underground disaster tourism market, people begin buying knock off fashion bags that are actually faraday bags, hand written and drawn emerges as a desired art form, people begin listening to live music in the park, skateboard culture explodes as a non-electric form of travel, over adornment of facial presentation with makeup and jewelry, cotton, wool, and leather are seen as the most desireable fashion material.
Question Two	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	Authenticity becomes the threat and China begins developing counter insurgency TTP's towards authenticity. Zhang's action was the Fort Sumter moment of the War on Authenticity. Lots led up to this. But this was the canon shot that made this a war. Paranoia builds in the regime as the government realizes that the data centric bondage mechanisms are coming unmoored. Governments that have built hyper digital and hyper surveilled societies begin to realize that the greatest threat to their stability are humans -- humans are the malware in the system. The instability in China puts up the red flag that authoritarian regimes around the world should take notice. The global powers including the US have to make a decision about how they will respond to this new viral disease that attacks the underpinning of their authority, power, and economy.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	(The answers to these questions are inherent in our responses to all the other items in this worksheet.)
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?	
Question One	**PASTE HERE**
Question Two	**PASTE HERE**

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.		
We are looking at what has to happen to disrupt, mitigate and recover from the Authenticity Revolution		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	The US ability to grab power back by weaponizing authenticity.	The US Military which is loyal to the Constitution, not to the regime.
2	A strategic doctrine that establishes authenticity as pillar of democracy. Using canada as a cut out. It's canada that is defending the authenticity revolution. (it's just the u.s. channeling money to canada.) (do the canadian chinese immigrants serve as the sharp edge of the spear?)	
3	The US intelligence agency quietly supports the organization of Wanhong influencers in China	This is human triumphalism, not american or western triumphalism. who comes to zhang's protection?
4	The meme of logging off has become the greatest act of resistance and the collective action that is in favor of authenticity begins to and forces a reckoning with the Chinese regime with multiple possible outcomes.	
5		
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	The proponents of authenticity don't have access to the large ammounts of data on its citizens.	
2	The proponents of authenticity don't know what tracking and surveillance algorithms have been built.	
3	The proponents of authenticity don't know the capabilities of the Chinese government to deploy artificial influencers.	
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?		**WHO?**
1	The rights of citizens as it relates to privacy and surveillance cannot be an opinion it needs to become to become a human right.	
2	Digital addiction needs to be treated as a public health emergency.	
3	More research needs to be done to forecast the impact of individuals as multinational corporations becuase if the individual becomes the definition of a corporation than that errodes at the expense of citizens.	

4		
5	The cloud is not your friend. Never trust a computer you can't lift.	
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?		**WHO?**
1	The new church/state separation is the separation of humans and their data as a sign of a healthy democracy.	
2	You own your own data.	
3	We're not going to code our way out of this. It's about the humans.	
4	Lead the charge on defining what it means to be a citizen. (Global and local.)	
5	Reclaim trust. What is trusted information? What are trusted institutions?	

Team Members:	**Blue Chip**
Experience Title:	**Professionalization of Rumor mongering**
Estimated Date:	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 Slot)	
Speaker 1	Millenials and GEN Z will be 75% of the workforce...
Speaker 2	trust is super important; friends and social influencers most trusted
Speaker 3	"Weaponized paranoia" is a real threat
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	**1. Hermione -- Parents liberal; she got hooked early on Tomi Lahren and got hooked into far-right vloggers and causes, including white nationalist movements. Joins military. Comes back and works at Amazon and barely gets by. She was driving uber, until driverless cars took that away. 2. Hermione's brother -- Harry -- He was a lawyer doing on-line consultation for immigrants, until the 2026 order to ban all legal immigration and suspend existing cases.**
Where do they live?	San Antonio
What is the threat?	State driven disinformation campaign driven through highly trusted social influencers with an aim of destroying trust in election, ends up causing violence on both sides. Disinformation includes deep fakes and inflammatory allegations fueling a sense of a life-or-death political struggle
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Hermione-- She received from an influencer (Russia-affiliated) in her closed social media community a deep fake video purporting to present a democratic political group plotting to deputize immigrants and deploy them to confiscate guns from conservative militias that are seeking to "defend" poling stations. Hermione gets her AR-15 and heads down to a polling station identied in the video as ground zero for the democrats' attempt to rig the election. Harry -- Receives from an influencer (Russia-affiliated) in his closed social media community a video of militias at polling stations actually beating a woman immigrant who they accused of attempting to vote illegally and handing her over to ICE agents to be taken to a detention center. The video asserts that democratic voters are being taken to detention centers en masse. The video calls for off-line direct action. ----- Violence erupts at the polling station, with rival factions committing acts of violence. Democratic-leaning crowds mob the militia, leading Hermione to open fire, killing Harry and several other supporters. Influencers weaponize video to enflame tensions across the country, resulting in broad-scale violence in most states and deployment of the national guard.
What is it? 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?	
	The Adversary seeks to further destabilize the United States and foment widespread violence, so that Russia has greater ability to formally annex its former terirtories (that it has not annexed already)
What vulnerabilities does this expose?	

	1. Influencers become media without ethical standards (like journalistic standards) 2. Influencers are mostly funded by countries and companies 3. Humans are incapable of distinguishing deep fakes from reality 4. People have grown up believing (and being willing to act on) biased information, including distortions and deep fakes that support their views
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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?	
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	**PASTE HERE**
What is different and/or the same as previous e	Influencers no longer considered fringe or youth source of entertainment, but rather excepted as the predominant source of information. They are increasingly financed and influenced by foreign actors, which is broadly accepted or ignored as a new normal.
Question Two	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	Greater ability of foreign actors to use influencers to foment broad-scale violence that can quickly metasticize. Ultimately, the ripple effect includes the failure of the democratic system.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	Further weakening of cultural aversion to partnering with foreign powers (in the case of influencer-funded content); Further weakening of political imperitives to denounce influencers on the right or left, given the need for both parties to mobilize their base; Further weaking of media as a gatekeeper
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?	Attack/finish destruction of journalism's reputation as trustworthy
Business Models: What new business models an	Influencer as a profession. It is already being funded by advertisers
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? W	Advertising & governments
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?	**PASTE HERE**
	Further weakening of cultural aversion to partnering with foreign powers (in the case of influencer-funded content); Further weakening of political imperitives to denounce influencers on the right or left, given the need for both parties to mobilize their base; Further weaking of media as a gatekeeper
Business Models: What new business models an	**PASTE HERE**
	More open funding of american influencers by media organizations sponsored by hostile states

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.		
Gates:		
What are the Gates?	US counter-intel monitoring of malign info-operations; US legislation around foreign agents	
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Surveillance programs to identify foreign-State backed influence operations	
2	Fact-checking channels and platforms (although these are shown to largely be innefective currently, given propsensity of individals to engage in Confirmation Bias)	
3	Foreign Agent registration requirements	
4	Education for parents and youth	
5		
Flags:		
What are the Flags?	Increase in social media influencers openly expressing views aligned with foreign powers; closure of traditional news outlets, or continued adaptation to influencer-centric formats; increase in off-line activity, including violence, driven by influencer-amplified content; increase in social media content calling for violence	
List out what the Defenders don't have control over to disrupt, mitigate and recover from the threat. These things should have a significant affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Decisions of individual infuencers to partner with foreign governments (although defenders can try)	
2	Propensity of Americans to perceive the political environment as a zero-sum fight with extreme consequences for failure	
3	Disinclination of influencers to register as Foreign Agents (or perceive that they are indeed acting in that capacity)	
4	Challenge--Limitations on US government's ability to message to internal US audiences	
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?		**WHO?**
1	Increased study of affiliation of US influencers with foreign governments, and enforcement of FARA	DOJ
2	Crackdown on social media content that advocates violence	Platforms
3	Broad inclusion of social influencers in a campaign effort to promote tolerance and constructive dialogue	Ad Council; Influencers
4	More engaging, effective fact-checking that does not simply debunk claims made by the other side; must be delivered by trusted influencers who can also "police their own" by rebutting false claims on their own ideological side	
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?		**WHO?**
1	Wholesale reducation in influence of foreign actors in US social media	
2	Significant reduction of division amongst US social media tribes	

3	US political leadership emphasizing compromise and the ability to coexist and partner with those who disagree	
4	Public rejection of foreign influence or infleuncer partnerships, whether by politicians or social influencers)	
5	Rejection of disinformation used in smear campaigns by political leaders, including rejection of proxies	

Team Members:	**Green Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Hard to descern misinformation and disinformation
Speaker 2	Cognitive Ease
Speaker 3	Using information deliberately to influence: misinformation, disinformation, malinformation
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Cuacausian mom with infant child and SE Asian spouse, possibly experiencing post-partem depression, living in more rural parts of a college town, integrated into the permanant resident community
Where do they live?	Urbana-Champaign, IL
What is the threat?	Corona outbreak and misinformation about its spread by unknown state actors
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	After reports of the first US case, Sue hears rumors from other mothers than infants are particularly at risk and that the spead is wider than the governement reports. After seeing a breathless discussion on the view she begins an agressive online research effort that guides down serveral youtube and social media rabbit holes.
What is it? 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?	
	Everyone who shares a phyical space; Isolation, chaos, economic destablization; Market-building by corporation (especially foreign pharma concerns); They are frightened of US stablility and hegemony
What vulnerabilities does this expose?	
	Health info illiteracy; Trust mechanisms
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?
	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	**PASTE HERE**
	What are the broader implications of a threat like this? What might a ripple effect look like?
	The very beginning of the event for Sue is converstations with her mother-in-law in Cambodia. Mom tells sue about numerous personal cases of Corona that she knows about, but the Cambodian continues to insists there is no outbreak. Days later, after the first US case is announced, she begins to network among her friends, many of whom are also new moms. In those conversations, she hears rumors that children, especially infants are super succeptible to the strain, which is often fata. Soon after panelists on the View have a similar conversation. Meanwhile the mother begin to suspect that the government is under-reporting the spread. Based on her conversation with mom, Sue reinforces this belief among her network. Following up on that, she does search-guided internet reaserch that takes her into a threat-actor SEO propomoted youtube rabbit hole, claming that these conspiratorial beliefs are correct. As she shares this research with her network, fear and irrattionality spread. Eventually, kinetic solutions such as a self-imposed quarantine are proposed.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**
	Business Models: What new business models and practices will be in place to enable the threat? How is it funded?
	Instead of new business models, we focus instead on the negative effefts of existing business models. Ultimately many state and non-state actors will have financial motives to promote fear-based narratives about US outbreak response. Profit-motive in pharma; state interest in corporate shananigans; Search engine optimization; Investment pressures on online media operations to grow beyond sustainability
Question Two	**PASTE HERE**
	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?
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.		
Gates:		
What are the Gates?	Trusted/effective government, an effective vaccine, mitigating pre-narrative campaign	
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	effective risk communication	
2	traditional multi-source journalism	
3	laws that make misinformation on health crisis illegal	
4	effective international monitoring	
5	platform improvements that make seo harder	
Flags:		
What are the Flags?	Always a low level biological threat going on, fears over vaccines, reactions to propsed responses, disaligned incentives across differing governements and industry, political misinformation campaigns have worked.	
List out what the Defenders don't have control over to disrupt, mitigate and recover from the threat. These things should have a significant affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	lack of technology to stop an outbreak-tool for misinformation	
2	difficult to regain control of a narrative after it has been deployed	
3	hard to constrain user-directed internet reasearch driven by confirmation bias	
4	when the disease breaks out	
5	self-reporting	
6	compliance w/ medical protocols	
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?		**WHO?**
1	vaccine prep where approriate	CDC, pharma
2	deploy competence narratives	govt
3	communal global fact-checking infrastructure	govt, media
4	diagnostic discipline	doctors, hospitals
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?		**WHO?**
1	improve surveiillance worldwide	CDC
2	data sharing across digital diagnostic tools	tech, govt
3	AI-based diagnostics and vaccine production	DARPA, tech
4		
5		

Team Members:	**Blue Pawn**
Experience Title:	**What if a war happens and no one shows up?**
Estimated Date:	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 Slot)	
Speaker 1	Children born after mid-90s are most diverse in terms of friend circles and preferences. Both societal values and because of the digital tools available
Speaker 2	Bubbles are a major part of the current problem -- a broader community of sources helps protect against biases
Speaker 3	audio/video/Photo manipulation
PART ONE: Who is your Person?	
	LTC Smith, male, 45, 23 years of service in US Army, Recruiting unit batallion commander
NOTE: Remember to give as much detail as possible. 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?	Batallion Commander in charge of 500 troops. Mid-level manager responisible for recruiting for soldiers in Los Angeles
Where do they live?	Los Angeles USA
What is the threat?	Recruits are not signing up/backing our. Trust in the military as an insitiution has been eroded
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	LTC Smith has consistenly missed mission and is not able to provide recurits to the force. People do not want to join the military because doctored video / photos show that the Army is an "evil" organization. Potential recruits have grown up in a world as the reason of every military action has been undermines as a false flag or a hoax
What is it? 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?	
	Who Else: Son- Kyle Smith has been consistently influenced by foreign threat actors through targeted media. As a child Kyle wanted to be a soldier like his dad, now Kyle is having contentious arguements with his father about the military. It has gotten to the point where mom has ruled that discussions about the military are not allowed on the dinner table
What vulnerabilities does this expose?	
	force structure is dependent on the public will to join the military
	Forcing the US to rely on conscription, a less professionalized army, unhappy conscripts are introducing a large amount of insider threats to the force; Social media sharing continues to undermine recruiting capabilites. Vietnam dicontent in a digital manner
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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?	Catalyst Event: Russia invades Poland with video evidence of "little green men" invading Poland, but the Russian disinformation sources post videos that statesGermany has invaded Poland first. When Polish citizen journalists post videos of the Russian Invasion, competing videos show a German Invasion. Commercial sources try to take down fake videos, but it takes days for the videos to be taken down. Publically available information reinfoces a German invasion of Poland. It gets to the point where everyone "knows" that Poland was invaded, the US government wants to move forces against Russia, but is facing mounting resistance from the U.S. population. Overall there is a lot of fear, uncertainty, and doubt.
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)	LTC Smith's social media feeds sends a burst of information showing an invasion of Poland, competing narratives are reinforced by mainstream media. He doesn't know what or who to believe. He comes in the next morning and his office has been firebombed, his Company Commanders are calling with messages that a large amount of recruits have backed out. Local law enforcement is calling and requesting that he closes his offices due to the possiblity of violent protests.
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	**PASTE HERE**
Question Two	**PASTE HERE**
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	Gaming the "fake news" algorithms; Citizen journalists; Has to co opt mainstream media; citizen independent digital forensic investigator "bellingcat"; No physical barriers, but there will be lingistic differences; digital platforms; digital behavioral differences; time-based differences; preplanned accounts and profiles, realistic looking accounts.
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?	AI enhanced/manipulated video, photos, audio. Person-based interactive bots "aka weaponized customer service bots" that cannot be identified as bots. AI generated photo,video,audio. In VR, Real person creates digital clones to engage individual citizens.
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?	
Question One	**PASTE HERE**
	Business Models: Chat bot development for customer service. Chat bots now learn to engage with people to move them from one psychological state to another. Funding: Commercial
Question Two	**PASTE HERE**
	Ecosystem support: A blurring of the lines of the grey space, a state of constant online warfare. Hidden Foreign VC funding into promising information technology firms. Hidden VC funding into influencer based entertainment. Anonymous donations to web-based funding accounts of "citizen activists / journalists".
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.	
Gates:	
What are the Gates?	

List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Digital Resilience Campaigns	industry collboration with government
2	Entertainment based fact-checking programs (for both the left and right)	entertainment industry
3	Classified Information (release of critical information)	Government
4	Unplug the internet (maybe)	Government
5	Content censoring - similar to Cristchurch shootings	Government
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Network Connectivity	All
2	VC Funding Streams	Industry
3	Worldwide political situation	Government
4	Citizen mesh networks	Citizens
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?		**WHO?**
1	digital resilience campaigns	government / industry
2	slowing down the 24 hour news cycle	industry
3	increased funding / authorities to inform population	government
4	Confirmed internet persona system	government / industry
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?		**WHO?**
1		
2		
3		
4		
5		

Team Members:	**Brown Chip**
Experience Title:	**Environmental Disaster**
Estimated Date:	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 Slot)	
Speaker 1	Participatory parenting
Speaker 2	Confirmation Bias
Speaker 3	"platforms" content/atomic unit
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	31yoa college graduate San Diego State male (Tom), A data scientist with NOAA (GS12), single no kids, live in boyfriend (Jackson), environmentally peaceful activist, inclusive attitude, liberal leanings, not religious but respectful. Polite but is stressed out about the world around him. Financially secure but not wealthy.
Where do they live?	San Diego, CA - suburbs
What is the threat?	A hurricane made landfall in the Southern California area (event) threat is adverserial advantage of the event.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	The San Diego area experienced severe flooding and was unpreppared to handle the devastating effects. However, a battle of narratives has emerged that conservatice data scientists do not attribute to climate change (el Nino) as opposed to his knowledge that the event is directly attirbutable to human created climate change. His boyfriend was in a coma because of the storm.
What is it? 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?	
	Tom is reading counter articles while in the hospital with his partner. Coal and Oil companies are blamed by some parties for the actions in San Diego. In Toms mind blood has now been shed by events in San Diego. The Navy has become the largest oil consumer in San Diego as the turn of the decade saw an unprecidendent US military buildup with appropriations reaching $1 trillion. Russia sees opportunity to engage in environmental terrorism by stoking the flames of divide in the U.S. after a major weather event.
What vulnerabilities does this expose?	
	Tom now has a personal life experience effecting his judgment. Tom recieves targeted information that he is interested in (fake news clippings, oil companies and the Dept of the Navy) exposing the hypocrapsy. George a college of Toms at NOAA disuccess freely his disdain for environmental policies and consistently references articles he reads discussing scandles in environmental groups such as Green Peace and Sierra Club. In conversations between George and Tom, George disguises his conversations as "some people are saying this" so we need to deal with this.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	

Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	What will the person have to do to access people, services, technology and information they need?
	Tom is living out of a hotel due to extreme flooding. Internet services are poor at best, Jackson remains hospitalized from injuries sustained from the storm. Work is only partially reopened.
Question Two	What are the broader implications of a threat like this? What might a ripple effect look like?
	Tom becomes violent and simultaneously steals confidential data from NOAA. Tom chooses to steal the most compromising data points of limate change and has not yet decided to do with the information.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?
	Tom is exposed to indiscernable deepfake. Micro targeting has now advanced into nano targeting. customized narratives for an audience of one. Automated generation of customized narratives for an audience of one. They know because of Toms social media posting that he is likely very upsent (Jacksons' hospitalization) Tom now has alot of energy to work out. The adversary picks this moment to launch a specified target package on an emotionally exposed person.
Question Two	Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?
	The adversry has to appear as coming from within the same organization/community the example here is a nomially peaceful environmental group moving towards violence.
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.		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	NOAA has an OPSEC program to help secure non-NOAA employees lives. All businesses have a valued desire to assist in securing their employees personal lives.	
2	The City of San Diego has a more informed emergency management plan based on environmental factors outside of earthquakes.	
3	An organization has a rapid response team to illuminate false information feeds after major events or drown out	Red Cross
4	The government develops counter methods to target individual bad guy actors.	
5		
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Amazon has developed an advanced AI that propagates information building based off a persons internet personna (social media, spending habits, website views, email correspondence and alexa listening.	
2	Services that are damaged in the San Diego area have degraded delivery mechanisms.	
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?		**WHO?**
1	In 4 years we identify weather related threat areas that could allow local municipalities (state and local) to plan for the unexpected.	
2	Most companies invest in operational security at work and at home.	
3	The US has developed better ecomomic levers to pull to influence adversaries.	
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?		**WHO?**
1	Getting Russia to stop is the most important thing we could do. Enter into an agreement with Russia to get them to stop IO diplomatic actions STAR Treaty.	
2	International norms have been established on the internet so that nation states have better understanding of what is expected with actions and counter actions.	
3	DSCA comforability in cyberspace	
4		
5		
Russia is the guy yelling fight fight fight in a riled up crowd		

Team Members:	**Orange Pawn**
Experience Title:	
Estimated Date:	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 Slot)	
Speaker 1	Self organization takes place now in cybersapce because of the limits of the terrestrial space.
Speaker 2	critical thinking, education
Speaker 3	Traditional warfair being applied to infomration: Techniques, Tactics & Procedures
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	Dr. Connie, obstetrician, performs abortions
Where do they live?	Austin, Texas
What is the threat?	AI driven deep fake
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	The deep fake videos have gone viral as fact across IoT of Connie performing an illegal abortion. Control of both houses of the U.S. Legislature are up for grabs between Democrats and Republicans. Protests between opposition groups are occurring in front of the clinic where Connie works, both virtually and physically based on beliefs that the videos are true. Second order effects cause mass violent confrontations between opposition groups and local/state first responders are overwhelmed. Governors declare marshall law, deploy the National Guard, and the President signs executive order shutting down networked platforms. These same platforms are used to organize political support for Connie's advocacy group (PP) at the polls. Platform shutdown denies government information organizations the ability to communicate the videos fakeness to the mass (public diplomacy).
What is it? 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?	
	A swarm of AI driven deep fake videos used as part of a nation-states IW campaign against the U.S. Connie's family is doxxed, leaving her family, co-workers, and friends vulnerable to the retribution of anti-abortion activists. The want sow mass chaos and polarization to distract the U.S. while attacking a neighboring country.
What vulnerabilities does this expose?	
	Dependency on networked ways of interacting, devices in the middle of transactions
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	
Questions (pick two)	
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?	
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	**PASTE HERE**
	What is different and/or the same as previous events or instantiations of the threat?
	Previous deep fake attacks used political/emotional themes for political advantage and discourse. This attack uses swarms of specifically developed deep fake videos that target hundreds of American political organizations most in conflict with one another.
Question Two	**PASTE HERE**
	Previous deep fake attacks used political/emotional themes for political advantage and discourse. This attack uses swarms of specifically developed deep fake videos that target hundreds of American political organizations most in conflict with one another.
	Connie sees herself performing an illegal abortion that never actually occurred. She has warrant for her arrest and there are voilent protests occuring between groups on both sides of the abortion issue outside of the clinic where she works. She is afraid to show herself in public. She has been doxxed and is receiving death threats from angry anti-abortionists. After the networked platforms were shut down, the general public remains uninformed about the authenticity of the videos. The nation-state enacting the attack simultaneously invades a neighboring country the U.S. has a security agreement and obligated to defend. The president is hesitant to respond militarily with an uninformed American public.
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)	
Questions (pick two)	
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?	
Question One	**PASTE HERE**
	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?
	AI driven deep fake videos are already demonstrated in the community and drone swarming is getting exponentially better. Combining both conceptually to form a powerful IW weapon.
Question Two	**PASTE HERE**
	Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?
	Academic/proprietary research on a global scale, nation-state theft of intellectual property, and the use of cyber proxies by nation states. Sources of funding motivates technological support betwee all parties within the nation state.
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.	
Gates:	
What are the Gates?	

List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Education	
2	Regulation	
3	offensive, defensive, and exploitive cyber capabilities (local, state, and national)	
4	alternative communication mediums	
5	funding and counter-funding/sanctions	
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	Research and Development	
2	organic funding and resources	
3	ideology	
4	Propaganda	
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?		**WHO?**
2	Educate the masses on responsible consumption of networked information	
3	Invest in R & D to detect AI driven deep fake and swarmed deep fake attacks	
4	Legislation to regulate who can post online content. Private citizen can post to friends network and credentialed journalist to mass media sources.	
5	Legislation to regulate who can post online content. Private citizen can post to friends network and credentialed journalist to mass media sources.	
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?		**WHO?**
1	Certified and educated disinformation specialist/engineers	
2	Advanced automated/AI driven counter-disinformation systems	
3	Accepted processes/laws governing the posting of mass media content and private citizen limitations to immediate social networks (professional/personal)	
4	Continue to foster business environment that encourages posting of trustworthy content	
5		

	https://qz.com/1165775/googles-voice-generating-ai-is-now-indistinguishable-from-humans/
Team Members:	**Red Pawn**
Experience Title:	**The social network strikes back**
Estimated Date:	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 Slot)	
Speaker 1	They value diversity and want to create more equitable society & environment
Speaker 2	Things are subtle:memes, not quoting sources, complexity of language, signals&signaling, rhyming as away of signaling meme, playground bullying with machine learning, signals get the confirmation bias going
Speaker 3	Rise of deep fakes
PART ONE: Who is your Person?	
NOTE: Remember to give as much detail as possible. 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?	An elite technology/new media executive named Mark; his community is tech executives, technologists, and wealthy people in San Francisco
Where do they live?	San Francisco
What is the threat?	Congress attempts to regulate the big tech/social media companies. Regulation fails and conspiracy theories circulate disinformation that the tech companies were manipulating socal media in order to kill regulation. Radical extremists on both sides accuse technology companies of engineering social outcomes that are dispicable. Deep fake videos circulate that supposedly show tech executives having conversations where they are discussing how they manipulate the public. This generates a broad public resentment of tech companies and extremists start assassinating technologists. Several tech CEOs are killed or die under questionable circumstances. This disinformation is circulated both by domestic extremists but also by malign foreign actors.
Briefly describe how your person experiences the threat (The Event) and possible 2nd/3rd order effects.	
	Mark is fighting massive PR problems and has received thousands of death threats. Conspiracy theories spread on 4Chan that Mark is part of a child trafficking ring for elites. Then a video is released purporting to show him having sex with a young girl. He denies it and claims it is a deep fake. Then additional videos emerge, some showing other tech executives. Police raid Mark's house and find child pornography on his computer (which was planted there by hackers). Tech company stock prices are tanking. Mark hears on the news that a warrant has been issued for his arrest.
What is it? 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?	
	Extremists want to keep the tech companies from engineering social outcomes they don't like. Foreign actors are trying to cause social discord and undermine our tech sector and economy. One hacker group is actively trying to foment a civil war in the US. Extremists are frightened of tech companies enforcing diversity / hegemony. They see a "white guy problem" where small numbers of people at tech companies are coding apps/AI/algorithms that incentivize certain behaviors (yoga, drinking smoothies) but disincentivize other behaviors (not-vaccinating your kids, driving a pickup truck). They see this as techno-authoritarianism. Foreign actors see tech and innovation as the source of US power and are afraid of competition and US tech dominance. They are also afraid of the power of tech companies to enforce/incentivize US (or white guy) values. The civil war hackers want to spark a hot war that they think "their people" can win.
What vulnerabilities does this expose? The amount of data collected about an individual by tech companies (and available for sale to anyone) is enough to generate strong predictive factors about most subjects and behaviors.	
	Deep fakes are effective because once you see something it is very hard to be convinced it isn't true (cognitive friction) and people are disinclined to believe a message that counters their own bias (cognitive disonance). Expert forensics of deep fakes after the fact are too late, not persuasive, seen as part of the conspiracy. People are tried in the court of public opinion - once a credible accusation of child porn is made, people judge and ignore any trial or additional info. State sponsored actors can probably hack anyone's computer.
PART TWO: Experience Questions (from the perspective of "the person" experiencing the threat)	

Questions (pick two)		
"The Event" - How will your person first hear about or experience the threat? What events or actions led up to it?		
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	**What are the broader implications of a threat like this? What might a ripple effect look like?**	
	Nobody is safe from slander, fake videos, information campaigns anymore. Societal trust goes to zero. We enter a post-truth world. The tech CEOs might get together and try to develop a unified solution. They might censor more content on their platforms. They could energize lobbyists and Congress to defend them. There could be a self-reflection by the tech companies where they agree to stop the "white guy problem"; they will do risk modeling to find knock on effects of new technology; they will include a multistakeholder group in all decisions about incentives/apps/algorithms. Perpetrators could see success and then move on to other groups, lilke politicians. Could spark a civil war Could use his social platform to go on the information offensive. Might unmask some people who were speading disinfo and give the information to law enforcement. If trust in law enforcement and government is too low, might engage a team of investigators to find the perpetrators and then have a team of hackers and info warfare specialists hack them or dox them.	
Question Two	**Where and how will the person connect and communicate with others? (family, aid agencies, federal, state and local authorities, professional network)**	
	Probably will call the FBI. Hire a group of private investigators to generate evidence. Will contact his Congressman Have a difficult conversation with his wife; convince her the accusations are not true. Family and friends also. Might send messages out through his social network. Wont know who to trust - could be a rival company trying to undermine them.	
PART THREE: Enabling Questions - Adversary or Threat Actor (from the perspective of "the party" bringing about the threat)		
Questions (pick two)		
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?		
Question One	**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?**	
	The technology to create deepfakes is not controlled or monitored. These types of dirty political operations would need to be normalized/enabled in the US by domestic actors. Malicious foreign actors would need to be prepared for retaliation by the US, including military action. Malicious actors need to remain hidden from law enforcement Countries like Russia might be promoting this information and videos on mainstream media	
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/criminal elements must the Adversary or Threat Actor team up with?**	

	Different groups are cooperating toward the same goal of attacking and undermining the tech companies without formal cooperation. They are riffing on each others memes and messages. State sponsored actors take the opportunity and send deep fakes videos and conduct hacks as targets of opportunity. There need to be a lack of circut breakers that prevent this kind of uncoordinated actions toward the same goal	
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.		
Gates:		
What are the Gates?		
List out what the Defenders (government, law enforcement, industry, etc) 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.		**WHO?**
1	Industry can change the virality of information and slow the movement of disinformation on their platforms	Tech industry
2	Congress could re-evaluate rules on free speech, difference between satire and slander; fair use of public footage	Congress
3	Industry could be inclusive in developing algorithms so a diverse group of people determine what apps and tools are incentivizing for	Industry
4	Congress or industry could restrict the spread of deepfakes technology.	Congress/industry
5	Industry and/or government could create new norms around the use of AI / incentivizing algorithms	Congress/industry
6	Could get rid of anonymity online	Congress
7	Could require data provenance - the origin of all data is known	Congress/ industry
8	Public education so people are aware of deep fakes and don't believe crazy videos (photoshop has been a	Public/government
9	A non-profit social network that stifles information operations, protects user data and expressly supports d	NGO?
10		
Flags:		
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 affect on the futures you have modeled. These are things we should be watching out for as heralds of the future to come.		**WHO?**
1	First compelling/ convincing deepfakes video created	Tech industry and a malign actor
2	Successful distributed network information attack: multiple networks of actors - not necessarily ideologically aligned - attack the same person/company/organization without any explicit coordination, but operating toward the same goal of disrupting/destroying the target	Many
3	Level of societal acceptance or disbelief in disinformation/deepfakes	Society
4	Insular groups of technologists create apps that incentivize certain behaviors (yoga, wheatgrass smoothies) and disincentivize/punish other behaviors (pickup trucks, listening to rap music)	Industry
5	Proliferation of social credit scoring systems - companies are all sharing scores they generate with each other (like how marketing data is shared now) and so your scores follow you throughout life and incentivize/disincentivize your behavior. And since the scores are private sector, plentiful and ubiquitous, they are very hard to avoid and correct	Industry
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?		**WHO?**
1	Pro-democracy/pro-privacy norms and principles around AI and social scoring/incentivizeing systems are developed, widely accepted and used across the technology industry	Industry/ education system/ in partnership with government
2	We achieve herd immumity for deepfakes so people are skeptical (but then people will be less likely to believe real videos of misbehavior); a well produced deepfakes video is disbelieved by an overwhelming % of the population	
3	Interactive PSA program that shows people videos and then they vote on whether it's real or not.	
4	A public/private partnership that can quickly identify disinformation campaigns and contain them before they go viral; an international CERT network for counter-disinformation; government can't do info ops against US population per EO 12333; so this would have to be private sector	industry
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?		WHO?
1	Develop technologies for real-time detection of deep-fakes	industry; government
2	Eliminate most anonymity online for public brodcasts	industry government
3	require content provenance so you can determine the original poster of most content online	industry, government
4		
5		

Appendix 6

POST ANALYSIS

The information found in the following pages is raw data and has not been spell checked or edited in any manner.

	Round	Team	Round One - "Summary"	Round Two - "Meaning"	Round Three - "Novelty"
	1	Black Chip	Female (Anna) (Cuban) technologist w/ expertise in "exo-psychology" - tweaks people's brains on Mars mission. Ops (One Planeters) want humans to remain on earth - they want collapse of colony. Eveyone on the colony walks outside without suits! OPS shape Anna's non-work reality exposing security and social vulnerabilities. Target back channels with corp competitor, hacking family to destabilize. GATE: Hardening against psychological manipulation	NO FA - extremists use Disinformation to target specific scientists and family as well as colonists to manipulate	Extremists (nano target) - NANO
	1	White Chip	Male (Latino) Texas holding referendum to suceed from US. Alt right and left are inflaming identity politics. The break will have economic and repercussion on minorities in TX as well as on the souther border. Male is a lawyer and his clients ask for new representation from person who is a "New Texan" Foreign entities fueling the break to create freedom of movement in Latin America. Puerto Rico, Somoa and Hawaii no longer trust US and pacific northwest climate radicals want to split. Mormons look to take pre-emptive steps. FLAGS: popularity of constitutional crisis and increasing conflict between local and national law enforement. Lack of recognized experts local and national media facilitating local echo chambers to be exploited by bad actor. Adversary works directly with alt right and left - deligitimizing national conflict resolution. Bot activity. Racial tension in states and schools. Community level conflicts. GATES: Info, facts and narrative concerning common benifits of domestic and international leadership.Actively work to discredit alt right and left. Tech to identify algorthmic manipulation and flag mis and dis information. New ways to deal with conflict resolution	NO FA - tribalism is heightened by Disinformation - no truth - ANTI-FEDERAL	Anit-Fed and tribalism break up US - WORST - NO FA
	1	Blue Chip	Male (Republic of Srpska) Sasha. Influence politicioans uses weaponized mems to drive and promote conservative/right - memes kick off self sustaining cycle of violence against minorities and rejection of western democratic values - USA and UK weakend influence. Russia becomes arbitrator for new leaders across Eastern Europe, South Am and South Asia. Nationalist leaders and malign media narratives play on ethnic tensions. Sasha sees meme about violence on Serbians from Bosnians and socail media call for violence. FLAG: social media application and closed platforms coopted by govnment networks.	FA undermines US/UK influence - uses ethnic tensions to incite violence	FA (kinetic violence) WORST (ethnic) US weakened in Europe - NANO
	1	Green Pawn	Female (Lily) single mother and small biz owner. Iowa. Small town. Corporate entity that is the agent of a foreign state wants farm. Lilly's is targeted personally. Her husband is influenced to leave her and influence in local town and church makes people questions Lilly's influence. Foreign government wants to ruin her life, get the farm land/IP, obtain her growing techniques and technologies either to utilize for their own corporations' operations or to bury to maintain the status quo. (Carol) foreign agent married George and has influence in local chuch and community. Lilly's kids affected social media and her bank account and driver liscence are disrupted. FLAG: personalized targeting directed at person and family members in different ways.	FA uses business entity in the US - micro targets citizen and family to break up family and discredit citizen in community (church) Digital and physical FA influence	FA/Bus (digital+physical manipulation) - NANO - BUS
	1	Purple Pawn	Female. Yuma AZ. Chaos and breakdown of economic and socail order. lack of jobs (structural unemployment) and opportunity, impowerished neigborhoods (lack of services, fresh food, low quality public space, leading to lack of security). This leads to desire for authority, someone to try to fix it as well as public health crisis. Uncertainty leads to overthrow of government, breaking down food supply chain. Martial law and isolationalism. Border wall is digital but with tunnels underneath. US citizens occasionally cross to Mexico for unregulated healthcare services and to smuggle in medication. Children typically grow up with a single parent or grandparents even if parents are living in the same community. they have arcieved confusion and fear. Given lack of resources, social trust and relatiosnhips have broken down. Decline of US incluence in global everything (political, economic, scientific, innovation, military). This leads to international power vacuum and free for all for autocrats. Lack of values (its declaratory, not lived), communication& discussion space, aplified by shallow and superficial mass comms platforms	FA uses economic and social order breakdown. ADVANTAGE - lack of resources, social trust and relationships break down. Globally US influence declines creating a vacuum	Economic circumstances leads to breakdown FA can step in on global stage
	1	Grey Pawn	Gen Z - digitla native Online meme-based Texas secession movement based on disputed 2028 federal election results and increasing divergence from "coastal" zeitgeist - Mobile media balkanized by aggressive filter bubbling; narrow narrative frame; anti-federal government sentiment; guazy nostalgia - localism - loss of federal gov counter narratives - computational amplification with A/B teasting - GATE Feneral government counter narrative , skeptics	FA uses Texas secession stemming from 2028 election contention and internal between right and left factions - computational amplification with A/B testing - anti-federal sentiment	FA w/ Anti-Fed (nano targeting) - WORST - NANO
	1	Orange Pawn	(female) Asian-American Journalist - LA - works for Chinese business media company - friends are diverse but family mostly Chinese - She has been asked to write a series of damaging articles (information both true, but damaging and untrue) about Amazon with the intent to influence its stock price (destroy investor confidence) so that it needs to sell to China, who will then have access to all consumer data and cloud-based web servers. Agreements Amazon has with DOD, etc., other government agencies, are now potentially available to China. The adversary wants to achieve technological, financial and intellectual property, as well as leverage over the US govt. The instruments of national power via information (technology, IP, consumer data) and economics. Consolidation of cloud-based services, the ownership by corporations of massive amounts of customer data, the stability of ths US stock market; Chinese acquisition of Amazon as a result of market chaos partly induced by Debbie's articles would further exacerbate the technological off-shoring of US IP and tech know-how; and also expose the US government to massive amounts of government information/data now being controlled by Chinese government (all the government services that run through AWS, including massive amounts of US DOD data and communciations)	FA uses US business entity uses US journalist to for misinformation about Amazon, affecting stock price allowing FA to purchase to gain technological, financial and IP superiority	FA + BUS - use economics to destability Fed
	1	Brown Chip	(female) hispanic 28 - peaceful split up of the USA into Red and Blue America via ballot propositions exposes the exterme polarization of the USA. Ms. Doe who leans toward Blue is worried if her state goes Red - lack of federal funding for local services and loss of confidence in economic drivers	R/L tentions lead to peaceful split up of US via ballot proposals - NO FA	Anti-Fed (peaceful split) WORST (NO FA)

*	1	Black Pawn	(female) Penelope San Francisco - teenage girl is finishing high school who is coming of age in a time when there are no certainties of "truth," and there's no "off." She's been swayed her whole life by narratives that are informed by half or false narratives. She's never really developed her own point of view, spending more time reacting to input rather than shaping it herself with original thought. She's looking at what's next for her path once she's completed high school. Her sense of truth has no boundaries, no guidance, no foundation. She has lived most of her life responding to memes, stories, narratives that were fed to her, without guidance and practice on how to analyze, interpret, and internalize what it means to her. Most of her education has been through user-generated, online, real time content. Throughout her life, she's experienced the continued development of deep fakes influencing major societal outcomes. Facts blend with fiction, and she can't tell the difference. Given that Penny has had so little practice developing her own voice and argument, she suffers from depression and massive self esteem issues. She's lacked role models who demonstrate a measured and thoughtful approach to engaging wtih the world. As she prepares for adulthood - for launching from her family's care - she's rutterless. In desparation, she "forces" causes on herself for direction, but snaps back into depression when she can't find authentic connection. The tech companies are already doing this - they are creating addition devices, fueled by addictive "drug-like" experiences. This is very little regulation or self-policing of the development of these potentionaly destructive devices. The government is woefully behind in understanding the true nature of this emerging threat, and in many ways, complicit in furthering the threat. Scientific studies take too long to come back with conclusive guidance and evidence on the impact of this relentless input on the developing brain. FLAG: Ubiquity of false info, opaque algorthims, rise of mnetal health problems, lack of college matriculation and drop outs GATE: informed parents and schools, peer groups, community. Goverment standards and industry (self) policing	NO FA - weakening of society via lack of truth, no point of view - via AI based education and meme based motivation - "The government is woefully behind in understanding the true nature of this emerging threat, and in many ways, complicit in furthering the threat. "	Weakening of society
	1	White Pawn	(male) China Xi Jinping - The Authenticity Revolution against the ancient regime that seemed so triumphalist in 2019 - China experiences The Authenticity Revolution. "Never trust a reality you can't touch." "Never trust a 'reality' that is multiplatform and multimedia." "I don't want to live in these fake cities." "Fake food." It's the calling bullshit revolution. A return to spirituality. (Confucianism nostalgia?) Status symbol: Shinola watches. Xi Mingze -- Xi Xinping's daughter, Handmade in China, Artisanal movement in China, Fake news/cities/jobs/communism/lives, "I'm taking the stairs" as an act of resistance, propaganda that you can believe in	NO FA - The Authenticity Revolution - as a reaction to surveliance and manipulation -	Truth as weapon
*	1	Blue Pawn	(female) 29 Erosion of narrative of western liberal democracy, regulatory failure, industries based on trust fail (example - medical) predicated by weaponization of narratives, weaken society, make less resilient --> Shock -- pandemic --> nation states fail. The Event: A catastrophic global pandemic is experienced worldwide placing a severe need on medical workers. Ten years of narrative campaigns has deteriorated trust in the health care system leads to ineffective treatment of the disease. Lack of trust	NO FA - Catastrophe (pandemic) mis/disinformation erodes trust in governemnt = ANTI-FEDERAL	Anti-Fed (catastrophe) - WORST - NO FA
*	1	Red Pawn	18 year old US about to vote - Chinese companies have bought USA text book companies and influence on AI driven educational system. Slowly and subtly putting pro China information. Their peers, family, community and country are involved. China wants a generation to have pro-China views and anti-USG views so they can take coercive military and economic action in E Asia and Africa. China wants Generation Z to think its not essential to live in a democracy; that the Chinese model is superior. China wants their international image to be positive; is afraid of being seen as manipulative/evil. They want the US divided and focused on internal sqabbles; they want democracies divided - When China takes action in Asia - two politicians on wants to push back the other looks to appease. Ripple effect is that its almost impossible to get Generation Z to change their belief. No longer support for promoting democratic values worldwide. Tolerance of authoritarianism. FLAG: Economic crisis weakens US to Chinese investment, AI manipulation technologies, China dominance in tech and data GATES: Government review of foreign purchases of US companies, mandate tools to identify manipulative actions in AI and tech, Congressional comission on data, info sec, online manipulation, parents educations	FA uses US business entity to use AI to manipulate education system - youth becomes pro-China allowing FA to operate freely. Eroding from the inside	FA + BUS - use education to destability Fed
	2	Black Chip	(Male) retired military - Phoenix - unemployable - was a teacher - Helicopter parents choose certain AI tutoring systems that can shape their childrens' identities to fit a particular tribal norm, world view, or pathway to success. Some of these AI tutoring systems have been co-opted by the "wings" of politics (alt-right, alt-left, theological, etc) and are creating very distinct tribes who will not see eye to eye. Truth becomes only as wide as the tribe and the constructed identity allows. Pete becomes unemployable because he has an obsolete vision of what education is and his online identity (which is the only one that now matters) does not have the "credentials" to belong to a tribe. He is the "universal other". The "adversary" is the constant pressure from other tribes who are trying to "capture" the identities of impressionable children from other tribes. Constant war of all-against-all with the goal of shaping children's identities. Tribalism becomes the norm. FLAGS: pubic perception of federal gov,trust in traditional knowledge development fails GATES: adoption of safe AI, mandatory draft for unifyed purpose, valid 3rd party in gov, financial security of public school, discourse and disagreement acceptable	NO FA - erosion of truth leads to tribalism and ANTI-FEDERAL	Anti-Fed - WORST - NO FA
	2	White Chip	(Male) CEO of quantum tech company - While negoting with a tech company in Paris to leverage their collective S&T investment, a Deep Fake (real time teleconference manipulation) is empoyed by Finland to order a shift in partnership to move all the quantaum communication intellectual poperty a competitor in Finland. Security of communication, inadequete and obselete regulatory framework. Intellectual propery laws and legal framework are obselete and cannot keep up with modern business cycle and tech driven deals. Vunerability to semi-closed peer networks that have high trust but can have misinformation campaign within the echo chamber that is biased towards action. FLAGS: realtime deep fakes, intel community signal industril espionage GATES: Secure comunication netowrks and cooperation, education of limits and detection of deep fakes	FA uses deep fake to steal IP and technology in real time from BUSINESS	FA (steals Bus IP) BUS
	2	Blue Chip	(female) State driven disinformation campaign driven through highly trusted social influencers with an aim of destroying trust in election, ends up causing violence on both sides. Disinformation includes deep fakes and inflammatory allegations fueling a sense of a life-or-death political struggle. The Adversary seeks to further destabilize the United States and foment widespread violence, so that Russia has greater ability to formally annex its former terirtories (that it has not annexed already) 1. Influencers become media without ethical standards (like journalistic standards) 2. Influencers are mostly funded by countries and companies 3. Humans are incapable of distinguishing deep fakes from reality 4. People have grown up believing (and being willing to act on) biased information, including distortions and deep fakes that support their views FLAGS: influences partner with foreign govs, GATES: crack down on influences, fact checking - Political switch to coexist and partner, rejection of disinformation proxies	FA uses influences to destroy trust in election - population destabilized via deep fakes and narrative allowing FA to operate freely on global stage	FA created Anti-Fed - WORST

*	2	Green Pawn	(female) Lily's status in the community makes her a high-value target for multiple entities. Local energy and water firms are trying to buy her and George's farm for the land, as is multinational lobby SoyCo - which already has interest in most of the farms in the area, and whom Lily has spoken out against in the past. A corrupt group within an existing political party wants to gain voters, and has identified the mother, Lily, as a possible 'swing person', where if she were to openly and expressly support their presidential primary candidate they would win the seat. 1st: George seemingly abruptly leaves Lily for Carol, a younger community member who is also the daughter of SoyCo's U.S. representative. 2nd: Lily's farm, Smythe Soy, loses some (but not all) intellectual property via George abdicating with it and giving it to Carol, who, it becomes apparent to Lily, is an agent of SoyCo/PRC. 3rd: Tom (Lily & George's 13 year old son), is the subject of vicious cyber attacks, troll farming directed at 'befriending' Tom and directing him toward certain coping mechagnisms (as he is desperate for positive reinforcement amongst his peers), which has cultivated addiction through augmented reality to first online gaming and later porn. He is ostracized from his friends group at school and falls into a deep depression. Meanwhile, Lily is subjected to unbenownst to her, a personalized social engineering-based propoganda campaign pushing her to endorce the Soy Lobby's Presidential Primary Candidate. Multiple adversaries from all sides - Pickens Holding (wants the land), SoyCo (wants the land and to kill the Intellectual Property, and to silence Lily's advocating against them), PRC (major funder of SoyCo, wants to obtain the I.P. for use on a global scale, dominate U.S. Soy Industry), Soy Lobby & Presidential Candidate (want to obtain Lily's vote and endorsement in order to swing Iowa. SOCIAL ENGINEERING interconnectedness and online presence linked to personal and professional life - Counter misinformation mailitias - FLAGS: omnipresent advertising and self-directed AI bots, foreign goverments purchasing American farmland GATES: increased awareness and action from citizens an government	(expanded from GP1- FA uses US business entity to nano target citizens and gain control of business, land and discret person. Attack is across entire family.	FA + Bus (w/ physical element - Nano target) NANO
	2	Purple Pawn	(male) young robotics engineer. Non-binary community. Living digitally - lives in bubble as robots and online proves all contact. Instead of creating, discovering innovating and thus driving economy, they're in a bubble of their own making. However, all of this is controlled by extrernal servers that run autinomous decidsions (AI) with little considerastion for security of connections. Therefore, a man-in-the middle can easily take over running this life withjout detection, causing a meltdown with no social support structure to catch it. Automated communication and 'fake friends'. Influence those on social media to spend more time interacting with fake friends and then have the subject realize that he has distanced himself from his 'real friends'. This takes an emotional toll. Causing the alienation of social groups and minorities by soreading weaponized narratives about them. FLAGS: unregulated human like robots, corp use only digital comms, unregulated foreign entity on social media, social ties wither GATES: education on stepping back from tech, tech to backtrack all social media friends (non AI)	NO FA - erosion of citizens ability to interact, flourish - synthetic humans - alienation of social groups and minorities	Weakening of society
	2	Grey Pawn	(female) caucasuan mom with infant child and SE Asian spouse - Corona outbreak and misinformation about its spread by unknown state actors. The very beginning of the event for Sue is converstations with her mother-in-law in Cambodia. Mom tells sue about numerous personal cases of Corona that she knows about, but the Cambodian continues to insists there is no outbreak. Days later, after the first US case is announced, she begins to network among her friends, many of whom are also new moms. In those conversations, she hears rumors that children, especially infants are super succeptible to the strain, which is often fata. Soon after panelists on the View have a similar conversation. Meanwhile the mother begin to suspect that the government is under-reporting the spread. Based on her conversation with mom, Sue reinforces this belief among her network. Following up on that, she does search-guided internet reaserch that takes her into a threat-actor SEO propomoted youtube rabbit hole, claming that these conspiratorial beliefs are correct. As she shares this research with her network, fear and irrattionality spread. Eventually, kinetic solutions such as a self-imposed quarantine are proposed. FLAGS: lack of tech to stop outbreak tool for misinformation, disease outbreak GATES: deploy counter narratives, communal global fact checking, laws around medical misinforamtion	NO FA - Catastrophe (pandemic) mis/disinformation erodes trust in governemnt = ANTI-FEDERAL	Anti-Fed (catastrophe) - WORST - NO FA
	2	Orange Pawn	(female) doctor - Texas - The deep fake videos have gone viral as fact across IoT of Connie performing an illegal abortion. Control of both houses of the U.S. Legislature are up for grabs between Democrats and Republicans. Protests between opposition groups are occurring in front of the clinic where Connie works, both virtually and physically based on beliefs that the videos are true. Second order effects cause mass violent confrontations between opposition groups and local/state first responders are overwhelmed. Governors declare marshall law, deploy the National Guard, and the President signs executive order shutting down networked platforms. These same platforms are used to organize political support for Connie's advocacy group (PP) at the polls. Platform shutdown denies government information organizations the ability to communicate the videos fakeness to the mass (public diplomacy). A swarm of AI driven deep fake videos used as part of a nation-states IW campaign against the U.S. Connie's family is doxxed, leaving her family, co-workers, and friends vulnerable to the retribution of anti-abortion activists. The want sow mass chaos and polarization to distract the U.S. while attacking a neighboring country. GATES: Education for public about consumption of networked information, legislation and technology to regulate	FA and Extremeists - deep fakes used to expanded contentious issue (abortion) leads to violence	Extremists (leads to kinetic) - WORST - NO FA
	2	Brown Chip	(male) NOAA scientist - San Diego - natural disaster but boyfriend in coma and displaces him - nonotargeted deep fakes - radicalize him - Russia sees opportunity to engage in environmental terrorism by stoking the flames of divide in the U.S. after a major weather event. GATES: NOAA (employer) and local goverment resillancy, rapid response team to expose deep fakes and mis information during catastrophes	FA uses Catastrophe (hurricane) to nono-influence citizen and destabilize US	FA uses catastrophe to create Ani-Fed (nano targeting) - WORST - NANO
	2	Black Pawn	(male) President Crowe - Phoenix - education can be implanted - Higher ed is under attack everywhere. Student enrollment is down considerably. Faculty salaries and benefits need to be paid, so debts are rising, limiting investment in new research and teaching. State funding is down. Faculty are being picked off by industry. Research is being taken over by private industry. Buildings are empty. The biggest threat is irrelevancy, and ultimately solvency. What can you distinctly offer students, faculty, and ultimately society from a higher ed degree/experience. It also exposes students to questionable "education" - what are the quality metrics of what constitutes high value secondary education? If students go towards highly personalized education, they choose their subjects and sources. Are they verified? Are they based in in foundational knowledge? What are the standards? Students fall prey to "deep fake" degrees. FLAGS: Rise of private alternative degrees, culture shift toward, companies no longer value college GATES: Offer financial incentives, lower cost, watch enrollemnt	NO FA - loss of trust in education system erodes US	Weakening of society (education)

	2	White Pawn	(female) China Zhang logs on Monday and realizes that "logging off" has become a meme of authenticity that has spread virally. Subsequently she receives a hand delivered letter by one man in a black suit where she is summoned to meet with the Minister of Wanghong. Zhang didn't mean to become a symbol that would launch a revolution, she just wanted some for her secret life, but what she didn't realize is that she set off a red alert in the regime that triggered her team, handlers, and representatives to urgently contact her while she's off the reservation. She has cut off her data for the weekend. “All human beings have three lives: public, private, and secret.” (Gabriel García Márquez) Authenticity becomes the threat and China begins developing counter insurgency TTP's towards authenticity. Zhang's action was the Fort Sumter moment of the War on Authenticity. Lots led up to this. But this was the canon shot that made this a war. Paranoia builds in the regime as the government realizes that the data centric bondage mechanisms are coming unmoored. Governments that have built hyper digital and hyper surveilled societies begin to realize that the greatest threat to their stability are humans -- humans are the malware in the system. The instability in China puts up the red flag that authoritarian regimes around the world should take notice. The global powers including the US have to make a decision about how they will respond to this new viral disease that attacks the underpinning of their authority, power, and economy. FLAGS: public unaware Chinese gov access to data, ability to influence and use surveillance algos GATES: Weaponize authenticity - establish authenticity as a pillar of democracy, digital addiction seen as health emergency. The cloud is not your friend. Never trust a computer you can't lift"	NO FA - War on Authenticity fueld by public unaware of gov access to data, ability to influence and use of surveliance algos	Truth as weapon
	2	Blue Pawn	(male) 45 - military commander - recruiting officer - Recruits are not signing up/backing our. Trust in the military as an insitiution has been eroded - LTC Smith has consistenly missed mission and is not able to provide recurits to the force. People do not want to join the military because doctored video / photos show that the Army is an "evil" organization. Potential recruits have grown up in a world as the reason of every military action has been undermines as a false flag or a hoax - Russia takes action in Poland and uses disinformation and deep fakes to create uncertainty. AI enhanced/manipulated video, photos, audio. Person-based interactive bots "aka weaponized customer service bots" that cannot be identified as bots. AI generated photo,video,audio. In VR, Real person creates digital clones to engage individual citizens. GATES: Digital resillance campaigns	Erosion of trust in military (ANTI-FEDERAL) weakens US and allows FA to operate in EU using disinforamtion and deep fakes to cause a split in option/truth in the US	Anti-Fed give FA takes advantage to expand operations - WORST - WEAKENING
*	2	Red Pawn	(male) tech executives - San Francisco - Congress attempts to regulate the big tech/social media companies. Regulation fails and conspiracy theories circulate disinformation that the tech companies were manipulating socal media in order to kill regulation. Radical extremists on both sides accuse technology companies of engineering social outcomes that are dispicable. Deep fake videos circulate that supposedly show tech executives having conversations where they are discussing how they manipulate the public. This generates a broad public resentment of tech companies and extremists start assassinating technologists. Several tech CEOs are killed or die under questionable circumstances. This disinformation is circulated both by domestic extremists but also by malign foreign actors. Extremists want to keep the tech companies from engineering social outcomes they don't like. Foreign actors are trying to cause social discord and undermine our tech sector and economy. One hacker group is actively trying to foment a civil war in the US. Extremists are frightened of tech companies enforcing diversity / hegemony. They see a "white guy problem" where small numbers of people at tech companies are coding apps/AI/algorithms that incentivize certain behaviors (yoga, drinking smoothies) but disincentivize other behaviors (not-vaccinating your kids, driving a pickup truck). They see this as techno-authoritarianism. Foreign actors see tech and innovation as the source of US power and are afraid of competition and US tech dominance. They are also afraid of the power of tech companies to enforce/incentivize US (or white guy) values. The civil war hackers want to spark a hot war that they think "their people" can win. FLAGS: rise of enabling technologies, cultural acceptance of deep fakes, insular groups incentivising certain behaviour over other, GATES: Pro-democracy/pro-privacy norms and principles around AI and social scoring/incentivizeing systems are developed, widely accepted and used across the technology industry	FA and extremists use deep fakes and disinforamtion to taget business (tech) executives. Destabilize tech sector	FA and extremists nano target business destabilize tech sector/Fed - WORST - NANO

Label (goal of 7 +/- 2 labels)	Description/Definition	Indicators or Flags	Examples	Exclusions & Special Conditions	What is the dependent variable(s)?	What are the sample groups?
FA (Foreign Actor, Foreign Adversary)	Non-US entities who wish harm to US values, practices, standards				Degree of threat (is this probability or consequence = a risk factor?)? Timeliness of threat?	US actors vs non-US actors? Political vs. business vs. civil actors? Advantage vs. Disadvantage? Broad vs. Individual targeting? State sponsored vs non-state sponsored? Do our themes differentiate these samples groups?
Anti-Federal	Any person or party against the current establishment of government; does not have to be hostile, violent, or malicious					
Advantage	Creating an opportunity that takes away from other actors					
Business	Actors with the goal of furthering aspects of business advantage including profits, market share, intellectual property, etc.					
Nano	Targeting people at the specific and individual level					
Worst	Using the worst part of ourselves against ourselves					
Weakening	A created state or environment within the US that weakens or chips away at the entire US as it is currently structured and valued (e.g., education, secession from Union, children coping in society, prominence on the world stage, etc.)					
Mis-information is when false information is shared, but no harm is meant.						
Dis-information is when false information is knowingly shared to cause harm.						
Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.”