A Widening Attack Plain

Threatcasting Report:
Army Cyber Institute

Brian David Johnson

with other participants

Participants and Army Cyber Institute Overview

Participants

Chris Arney	United States Military Academy
Joshua Bundt	Army Cyber Institute
Erik Dean	Army Cyber Institute
Bill Cheswick	Founder, Internet Mapping Project
Chris Claremont	Author, X-Men
Alida Draudt	California College of Arts
Adam Duby	Cyber Protection Brigade, U.S. Army
Sean Griffin	USAA
Andy Hall	Army Cyber Institute
Steve Henderson	Carnegie Mellon University
Rhett Hernandez	Army Cyber Institute
Dan Huynh	Army Cyber Institute
Brian David Johnson	Arizona State University
Paul Maxwell	Army Cyber Institute
Fernando Maymi	Army Cyber Institute
Michael McDonald	Army Cyber Institute
Glenn Robertson	Army Cyber Institute
Gus Rodriguez	New York Police Department
Brian Schultz	Army Cyber Institute
Rock Stevens	U.S. Army
Rob Thomson	Army Cyber Institute
Natalie Vanatta	Army Cyber Institute
Carlos Vega	Army Cyber Institute
Clint Watts	Citigroup
Julia Rose West	California College of the Arts

Army Cyber Institute Overview

The Army Cyber Institute at West Point is the Army's and the nation's think tank for cyber warfare and the cyber domain. The ACI creates knowledge, builds public and private sector partnerships, and creates an entrepreneurial and innovation laboratory to focus investments. Positioned to establish and maintain relationships with the nation's economic center of gravity in New York City, the ACI directs and synchronizes efforts across the U.S. Military Academy in the cyber domain. The ACI collaborates with the U.S. Army Cyber Command and U.S. Army Cyber Center of Excellence to prevent strategic surprise and ensure the Army's dominance of the cyber domain.

Table of Contents

Threatcasting 2026: A Widening Attack Plain

Executive Summary

> *The year is 2025 and automation is pervasive. From clothing to appliances to self-driving vehicles, it seems there is an embedded computer everywhere. The benefits of the Internet of Everything are taken for granted by most, but not all. Mike is a frontline supply chain supervisor working at a regional distribution center near the port of Red Hook, Brooklyn. On a crisp autumn day, he would normally kill time at work by tracking the value fluctuations of the handful of stocks he owned. The artificial intelligence running the complex logistics apparatus makes for pretty boring days, but not today*
>
> (Excerpt from a Threatcasting Possible Future)

What follows this opening excerpt is a detailed future distributed denial of service (DDOS) attack launched via Internet of Things (IoT) devices on a complex and automated supply chain. The failures of security protocols and the management of AI in the digital domain leads to a physical weaknesses and ultimately to a kinetic dirty bomb attack on the isle of Manhattan. Modeled by experts across multiple domains this possible future then explains what needs to be done to disrupt, mitigate and recover from such a threat.

On August 2016, twenty-five participants from government, military, academia, and industry gathered for two days to participate in a threatcasting workshop to formulate possible future cyber threats. Threatcasting is a conceptual framework and process that enables multidisciplinary groups to envision and plan in a systematic fashion against threats ten years in the future. From a wide array of disparate research and data, the group started an ongoing process to craft a vision for the future of digital and physical security along with recommendations how the Army Cyber Institute (ACI) and the Army can take actions to disrupt, mitigate and recover from these threats.

The goal of the threatcasting and backcasting process was to first model future cyber threats as dictated by curated technology, culture and business trends while exploring the implications on the ACI, Army, DoD and wider participants (e.g. public and private organizations, academic, general public, etc.). Our second goal was to come up with clear next steps that the Army could take as an organization to get the combined positive future that we modeled, while avoiding any negative futures. Finally, this report and the exercise will provide a framework for thinking

about the future, so that organizations can continue to process new information and developments while staying true to the collective futures modeled.

Based upon the technological, cultural and economic shifts and advances in the next decade we begin to see an evolving threat landscape emerging. This new reality of cyber and data security can be seen as a widening attack plain. The attack surface in the future broadens out, including more people, increasing targets, and changing the very nature of security and threat.

The cyber threats over the last decade have mainly been isolated to "data only" threats, espionage, leaks and hacks. In recent years, the nature of these attacks have expanded to include micro-targeting, cyber-physical and cyber-kinetic attacks. In the next decade we will see a continuing widening of the attack plain.

As we look at the future of cyber threats, we must look beyond the current digital attack surface and see a plain that is far wider and exposed. The nature of hacking and cyber itself will become another tool or weapon that can be used alone or with more frequency as a blended attack. These blended attacks provide the most potential for devastating offense and increased complexity for the defense.

Future Threats and Actions

The threatcasting process uncovered multiple threats and necessary actions, the detail of which are contained in this report and its appendices. However from this data we have identified two broad categories of threats and actions that can be taken.

Threat: War on Reality: The Weaponization of Data and AI

Autonomous systems depend upon data to construct a model of the physical world. If this data is corrupted or deliberately manipulated, these highly automated systems could not be living in the same reality as we are. The information into these systems can be altered, falsified, spoofed and manipulated to not only affect the system but weaken or destroy it. The greater use of autonomy also means that this weaponized data can quickly move effects from the digital or cyber domain to the social, physical and/or kinetic realms.

Artificial Intelligence (AI) will be the backbone of these complex autonomous systems, allowing them to operate and make decisions. But the weaponization of AI also means that AI can be used as a part of these blended attacks.

At the same time, AI can also be used to monitor this expanded attack plain, looking for vulnerabilities and either prompting or taking autonomous action on its own. For example, an

attack might take place by a third party. A hacktivist takes down a system as a form of protest. But then a state sponsored or criminal network using AI could identify this un-associated action as it opens a window or vulnerability that they want to exploit. In this way a completely unrelated and unknowing actor could work to further the desired outcome of another party. AI and these highly automated complex systems become a key component in these blended attacks because the actors on their own will not be able to monitor the entire attack plain.

Threat: Efficiency is Easy to Hack: Vulnerabilities of Complex Automated Systems

There are few regulations that govern the use of AI and automation. Globally there is no norm or accepted practice for human oversight of these systems or how the "human remains in or on the loop." The biggest vulnerability of these systems is the very thing that will promote their use and adoption: efficiency. Market forces and business management reward efficiency, whether this is cutting costs or increasing production; both efficiency and productivity are highly valued.

As these systems undergo a wave of automation with efficiency as the driving factor, for threat actors these systems become increasingly easy to attack. Stated simply: Efficiency is easy to hack.

If the threat actor knows how the system is constructed, what it values and what it has been optimized for - then they can use both the weaponization of data and the use of AI to hijack and even use these systems as a part of the attack.

Additionally, these systems are designed with security as an afterthought, with a lack of understanding of the critical nature regarding the welfare and security of the country. In fact, many of these systems have not been designated as "critical systems", they have not been treated with the same severity and precautions for redundancy and security as other similar systems like the energy grid or water systems.

Action: The Need for Norms

There is a need for international norms, irrespective of cultural or social rules for the cyber domain. Unclear cyber boundaries, ethics, behaviors, expectations, and legislation need greater definition in order to govern national and international relationships.

In contrast to the physical boundaries of Nations, societies, and cultures, technology is designed to integrate across multiple domains. An international consensus or "norm" is required to

develop both rules to deal with “bad actors” and minimum standards for cybersecurity in technologies.

These norms or standards should span across policy, security, technology, and safety. Using a holistic approach, considering both the technology itself and its proposed uses. This will require collaborating with industry and academia to address all threats across the attack plain. Working with industry to explore “Go Dark” Plans (massive failures and outages) and the possibility of data security “Amber” style alerts.

Action: Living in the New Reality

The reality of the widening attack plain is that the Army and military cannot defend all of the digital, individual/social, physical and kinetic domains. Working with private industry, academia and the general public we all must first understand that we are living in a new reality.

The emergence of diverse future adversaries will force a change in how we imagine who they are as well as how they will operate. Over the next decade, it will get progressively harder to determine intent from actions as the attack plain is increasingly driven by the availability of technology and skills.

History shows us that these types of changes needed (such as behavioral, political, and tactical) start virally, across of number of domains and industries and then disseminate outward. Typically a “top down” strategic plan approach will not work. This calls for a new era of increased collaboration, communication and cooperation.

Implications and Next Steps

For many, future cyber threats seem unimaginable and insurmountable. This threatcasting report seeks to envision these threats and empower people and organizations to take action. These possible futures, based on facts and modeled by professionals, can dispel the myths and clear the fog for pragmatic, action-based dialogue. The report also lays out pieces of the strategy to dispel or allow recovery from the negative futures. While some of these actions rest in government hands, many of them must be adopted and executed within industry, academia, and society to be successful.

Introduction:

How to use this Document

This introduction is an overview of the document that follows with recommendations for how it can be used.

This full report contains both the analysis and the raw data collected during the threatcasting workshop held at West Point as well as the clustering and post analysis. The intent of this report is to be a stepping stone for further research on the findings and more specific and curated threatcasting sessions.

There are multiple ways that this report can be viewed and used. It is designed as a tool for readers who want multiple levels of detail. If you are interested in the entire process from start to finish please review the entire report. But if you simply need specific and concise windows into the project please review the following:

The Executive Summary: A short concise overview of the process and findings with pointers and notes to further information and detail.

Next Steps: An overview with details about the findings of the first threatcasting workshop and recommended next steps.

Appendices: Contain all of the raw research data that were used as inputs to the process as well as the unfiltered workbooks that were used in the West Point threatcasting workshop.

Threatcasting: Process Overview

Threatcasting is a conceptual framework and process that enables multidisciplinary groups to envision and plan in a systematic fashion against threats ten years in the future. The groups explore how to transform the future they desire into reality while avoiding an undesired future. Threatcasting is a continuous, multiple-step process with inputs from social science, technical research, cultural history, economics, trends, expert interviews and even a little science fiction. (Figure 1) These various inputs allow us to create potential visions of the future (a person in a place doing a thing). Some of these futures are desirable while others we would want to avoid. Then, by placing ourselves into the scenario, we can imagine what we need to start doing today, three years from today, and so on to empower or disrupt that future. We can also determine what flags (or warning events) could appear in society that indicate that we are traveling the path to this future.

Threatcasting is fundamentally different from traditional strategic planning and scenario building processes because it identifies specific actions, indicators and concrete steps that can be taken today to disrupt, mitigate and recover from future threats.

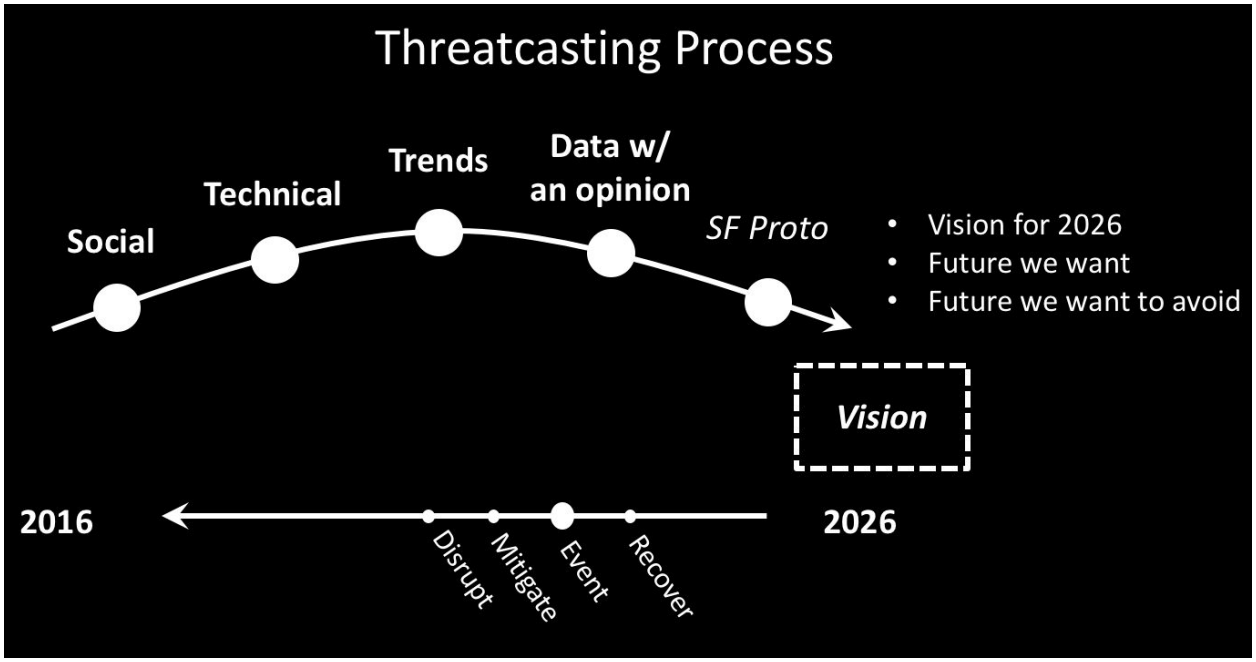

Figure 1: Threatcasting Process

The ACI hosted a threatcasting workshop on August of 2016 at West Point on which this document is based. It was an interdisciplinary and collaborative session to envision future cyber

threats ten years in the future. The ultimate goal was to produce a threatcasting report that explores cyber threats and cyber security issues that would empower research efforts and relationships across sectors. This report contains specific actions, external indicators and milestones that can be taken to disrupt, mitigate and recover from the threats.

This document will be shared with government, military, academic, public, private and corporate audiences. We will use it to foster conversations and dialogue with a wide range of audiences (to include military, industry, academia, policy makers, trade associations, law enforcement) with a diverse set of outputs (such as Threatcasting Reports, briefings, articles, podcasts, videos, and science fiction).

We feel it is important to bring together a wide variety of people and organizations not only to envision possible cyber threats but also to discuss what specific actions can be taken. The threatcasting process also allows for us to monitor our success, scrutinize the indicators and the success of the recommended steps to disrupt, mitigate and recover from these future cyber threats.

For many, future cyber threats seem unimaginable and insurmountable. This threatcasting report seeks to envision these threats and empower people and organizations to take action. These possible futures, based on facts and modeled by professionals, can dispel the myths and clear the fog for pragmatic, action-based dialogue.

The threatcasting process is founded on bringing together diverse multidisciplinary groups to model possible threats with data pulled from a wide variety of sources. Both the process itself and its outputs provide a knowledge base for decision makers across various sectors.

The iterative process of threatcasting will allow us to constantly monitor the success of the visions and make course corrections depending on the indicators and actions that have come out of the August 2016 workshop.

In the post-analysis of the multiple futures that were created, we do not look for a single future. No single future is correct. The power of the threatcasting process comes from the aggregation of these futures. We looked for clusters of threats, actors and trends. We also looked for areas and threats that were not identified in the session but that have been identified both other research and foresight work. Ultimately we begin to discern a set of insights and areas for further investigation. The August threatcasting workshop identified a collection of clear threats with interesting implications. Before we dive into these findings, we should review the research and data that helped us reach our conclusions.

How we got here…

We heard from experts in seven disparate areas: social, technical, economic, as well as data with an opinion. (See Appendix: Research Inputs.) We then used them as inputs to model the future. We split up into teams, synthesized these disparate pieces of research, and then shared the analysis of the inputs with the rest of the room. (See Appendix: Research Synthesis Workbooks.)

Finally, we broke up into these same groups and used a curated workbook to model a person in a place with a problem. The seven inputs (and some expert dice rolling!) guided our models for the future. (See Appendix).

We closed out the session for the day by backcasting those futures. We investigated the various gates and flags on the timeline between today and 2026 within those futures. The gates and milestones were things that the Army had control over; the flags were incidents and areas that the Army had no control over, but could have a significant effect on the futures we had modeled. (See Appendix).

The Research Inputs

A fundamental component of the threatcasting process is choosing the research inputs that will feed into the future models. At the start of the workshop, participants heard from subject matter experts (SMEs). In groups, they pulled together the key/interesting points that were discussed. An overview of this information is captured below (with the full presentations in the Appendix). These concepts then directly fed into the scenarios. For the August threatcasting session, we specifically chose the following areas of research to hone and better define the threats we modeled:

Social:

Steven L. Neuberg, PhD
Professor, Department of Psychology (Social), College of Liberal Arts and Sciences
Arizona State University

Neuberg explored the idea that the human mind's primary task is to detect threats and identify opportunities. As we model the future we must understand these threat and opportunity systems. Their calibration and outputs will be useful when doing long term forecasting and designing systems.

Human evolved threat management systems can be broken down in the following ways: Humans have multiple systems to detect threats. These systems are qualitatively distinct, they look for different inputs.

- Human self-protection systems
    - Disease Avoidance:
        - Humans have not only a physical immune system (that we all imagine when we think about disease avoidance) but humans also have a behavioral immune system (designed to anticipate viruses) that protects humans from coming into contact with disease so that the physical immune system does not have to be used. Effectively, it stops a virus from even getting into the system.
    - Social Affiliation/Status is another protection system we use. Human are social beings and our social nature matters to us and this imbue bias into the process of threatcasting.

    - When we model the future we also must understand the goals of the threat actors. What do they want to achieve? What are they frightened of? What are their aspirations and dreams?
- Short-term versus long-term forecasting
    - The mind has problems looking further out into the future
    - When we model the future, we need to understand our bias which may impact how we communicate the results of this work to multiple audiences. There will always be a short-term bias that derails long-term thinking. This cannot be avoided; it should be addressed, understood, and embraced.
- Historical Cues and Biases not diagnostic of real threats - the human brain has been around for a while. Embedded in our activities is a deep historical bias that we will pull from cues that served us for many thousands of years. But these historical cues (to what is danger) may not help us in the present and hinder us in the future. For examples:
    - Young lone men: Humans have an inherent fear of "outlier" men. These are young males that are not apart of our social system. Made lots of sense back in our ancestral history where coming across a lone male was dangerous. Living in a large society like the United States, this cue does not have the same diagnostic utility in terms of implying threat but we overuse it anyways.
    - Physical deformations: As a part of our disease avoidance system, humans also have a repulsion of deformities or abnormalities. In the past this might have been an indicator of disease. In present day, it can produce a strong bias against the different, injured or disabled.
- Smoke detector principle - When we were modeling the future and trying to come up with models and systems for avoiding threats we should think about the smoke detector and how it is designed as a threat avoidance system. For example:
    - A Smoke detector can make two kinds of errors.
        - Going off when there is no fire. (annoying)
        - Doesn't go off when there is a fire. (deadly)
    - In the factory, the detector is calibrated to go off valuing one error before the other. It is designed to go off more often than not.
    - This pushes us to ask some questions about our own systems for threat detection and avoidance:
        - What are the conditions and profiles and values we are using and that are imbedded in the system?
        - What are the trade offs?
        - What are we optimizing for (cost and benefits)?
- Vulnerability Perceptions - human perceive threats depending on the content of their current situation.

    - When we model we should consider the context when assessing vulnerability or threat level.
    - Broad ecology: when resources are scarce, humans feel more vulnerable and will react more quickly and harshly to threat stereotypes.
    - Threat management systems are calibrated by the vulnerability perceptions that we have in a given environment/context.
- Human opportunity management systems - not only should we think about threat avoidance systems but should also consider threat opportunity management
    - Does it make sense to design a system to detect threat opportunities? What are the cues for these opportunities? How do we process information about opportunities?
    - Opportunity systems as opposed to threat systems

Link to video: https://vimeo.com/178936588/88549c8b7a

Technical Research:

Brian David Johnson
Futurist and Fellow - Frost and Sullivan

Johnson explored that 10+ year out observations. Significant advances in technology and shifts in economies and culture are bringing about a new age of intelligent tools that are aware, can make sense of their surroundings, and are socially cognizant of the people who are using them.

Sentient tools are the next step in the development of computational systems, Smart Cities and environments, autonomous systems, artificial intelligence (AI), Big Data and data mining, and an interconnected system in the Internet of Things (IoT). These tools are “what comes next” and emerge from a base of computational, sensing, and communications technologies that have been advancing over the last fifty years.

The awareness of these sentient tools is not comparable to a human level of consciousness. They are not meant to mimic, mirror, or replace human interaction. These tools are designed for specific physical and virtual tasks that could be vastly complex but are not meant to replace humans. Conversely, they are meant to work alongside the human labor force. The rise of sentient tools will have a significant impact on the global workforce and education, leaving practically no industry unaffected.

Sentience is defined as the ability to perceive the world that surrounds us and derive feeling or meaning from those experiences. For a machine or tool, being able to derive meaning infers that the tool is capable of some level of perception, processing and thinking. In this case sentience is both the ability to sense the world around the tool but also to process, understand, make meaning and communicate with that world. To be able to effectively interact with that world, the tool needs to be socially aware of the person it is working with. It must understand the person as an individual so that it can more effectively communicate. (See Full Paper in Appendix)

Trends:

Fernando Maymi, PhD
Deputy Director, ACI

Maymi gave us a report out on the Tactical Ground Warfighting circa 2050 project. This work explored, for the Army, what trends could affect the future of warfighting that could dramatically change engagements. These areas included:

- Augmented humans
- Automated decision making and autonomous processes
- Misinformation as a weapon
- Micro-targeting
- Large-scale self-organization and collective decision making
- Cognitive modeling of the opponent
- Ability to understand and cope in a contested, imperfect, information environment

(Full presentation in the Appendix)

Expert Perspective:

Jamie Winterton
Director, Strategic Research Initiatives Global Security Initiative
Arizona State University

Winterton offered five general things to consider:

1. The Internet was constructed to push out data to as many people as possible. The Internet was never designed for security.
    a. Do we need to build a new version that has security and privacy?

2. We have a specific approach to security and hacking in the USA. We do not embrace hackers but other countries hire hackers.
    a. How could you put together a team of hackers to go on the offensive?

3. Who is being threatened? We need to understand all the threatened and threat actors that we involved.
    a. Need a wider range of possible actors for risk and vulnerability assessments

4. Opportunistic threat distortion. Consider threats and threat surface as they actually exist.
    a. The noise distorts the system
    b. When there is too much noise, we often address the noise but not the threat

5. Cyber peace - how do we design for cyber peace? Cyber war should not be our goal (though we wage it effectively and/or impactfully) but how do we set a goal to live in a cyber peace?
    a. How do we architect a world that holds cyber peace?
    b. Cyber peace must have security and privacy as a component.

Full video: https://vimeo.com/178932718/affb7a907e

Expert Perspective:

Sharon Rice
Vice President, Strategy - APICS
Global Supply Chain Expert

Rice detailed that a number of cyber attacks have been focused specifically on the global supply chain. This provides a number of different complexities and problems.

The first is that global supply chains are only as strong as their weakest links and all supply chains have weak links. Typically these weak links can be found in the fringes of the supply chain. Even if the majority of the system is secure, there will usually be a “mom-and-pop-shop” somewhere in the system that can take the whole system down.

Example: Target hack came in through the HVAC subcontractor.

Secondly, supply chains pose a particular threat because they are where the digital supply chain meets the physical supply chain. Also, these supply chains have a huge effect on global commerce and economic stability. If a supply chain is sufficiently hacked, then an entire country can be destabilized and hacked.

https://www.brainshark.com/apics/vu?pi=zGLz8Ul3czMdQ0z0&intk=230788048

Landscape Review:

Aaron Brantly, PhD
Cyber Fellow, ACI

"Tech 4 Terror and the Future of Jihad"
Brantly reviewed how terrorists can and will technology to gain political gain. His report gives us a well rounded view of the current threat actors (terrorists/hacktivists/state sponsored/criminals) as an input for understanding how to model them

The specific characteristics of these threat actors include the following:

- Threat actors are Digital natives
- Better informed about than ever before about state capabilities for defense
- Extensive understanding of using technology - have grown up with technology and are comfortable with exploiting its capabilities
- Problem is not geographically located. Because of highly networked systems, threats exist globally and can work together globally
- Networked and distributed networks of threat actors
- Threat actors have a plethora of information that has already been leaked
- Threat actors know how to take advantage of decentralized social networks for communication, training and recruitment
- Expanded digital tools
- Use of the Dark Web
- Technical ability of non-state actors continues exponentially over the next 10 years

Full video: https://youtu.be/5ow9IERcuX4

Expert Report:

CyberSecurity Futures 2020

Center for Long-Term Cybersecurity report on 5 potential scenarios for cyber security in 2020. These were used as a baseline for us to look out to 2026. Below is an overview of the report.

How might individuals function in a world where literally everything they do online will likely be hacked or stolen? How could the proliferation of networked appliances, vehicles, and devices transform what it means to have a "secure" society? What would be the consequences of almost unimaginably powerful algorithms that predict individual human behavior at the most granular scale?

These are among the questions considered through a set of five scenarios developed by the Center for Long-Term Cybersecurity (CLTC), a new research and collaboration center founded at UC Berkeley's School of Information with support from the Hewlett Foundation.
These scenarios are not predictions; it's impossible to make precise predictions about such a complex set of issues. Rather, the scenarios paint a landscape of future possibilities, exploring how emerging and unknown forces could intersect to reshape the relationship between humans and technology—and what it means to be "secure." (See Full slides in Appendix.)

Curated Inputs Bring Focus

As a part of the threatcasting process, we understand and embrace the fact that we cannot model all threats. It would be impossible in a few day session to model the entire future of cyber and digital threats. With this idea firmly in mind, we used the inputs described above to focus our threatcasting on specific areas. These were specifically chosen to explore how the areas might work together to create new combined threats that we have not seen to date.

The focus of these curated areas and selected presenters discussed concerns/threats, by design, to examine the following areas:

Supply chain disruptions and vulnerabilities (via Sharon Rice) was picked because of their cyber/physical nature, their global reach, and the economic and security effects of their destabilization.

Autonomous systems and artificial intelligence (via Brian David Johnson) was chosen because the nature of these technologies will greatly change the threat landscape both for potential offensive attacks and defensive activities. This new landscape will stretch across military, private sector and individuals (civilian, Soldiers, Soldier's families). By broad definition, autonomous systems encompass multiple technological advances. Particularly of note to this session were: shrinking computation power, smart cities and intelligent environments, autonomous transport (land, sea and air), autonomous manufacturing and data science.

We explored the use of artificial intelligence (AI) to enable these complex autonomous systems, but also for its ability to monitor and act inside of this complex hardware and software ecosystem. But more specifically we wanted to explore the possible weaponization of AI, using it as an offensive and defensive weapon.

All of these inputs and data points were used to model multiple futures and threat scenarios. The participants were divided into seven teams where they rolled multi-sided dice, choosing one component from each of the seven speakers. The combination of these seven concepts became the backbone for the future scenarios. In order to better articulate their vision, they described the future in the terms of a person in a place doing a thing and how their life was affected by the cyber threat.

Once we had modeled these possible futures, we explored what needed to happen to disrupt, mitigate and recover from these threats. Also as a part of the threatcasting process, we not only identified what the threats were but who was involved. This included who was involved upon the discovery of the threat and also who needed and would be involved in its disruption, mitigation and recovery.

In the post-analysis of these threats, we have constructed a vision for the future of cyber threats based on these curated inputs. We characterize this new threat landscape as: A Widening Attack Plain.

Threatcasting 2026: A Widening Attack Plain

Based upon the technological, cultural and economic shifts and advances in the next decade we begin to see a different threat landscape emerging. This new reality of cyber and data security can be seen as a widening attack plain. The attack surface in the future broadens out, including more people, increasing targets, and changing the very nature of security and threat.

The cyber threats over the last decade have mainly been isolated to "data only" threats or espionage. These types of threats are things like data breaches for "hack and release activities", intellectual property theft or criminal activities. Only in recent years have we begun to see the nature of these attacks change to include micro-targeting, cyber-physical and cyber-kinetic attacks.

Cyber Social Threat

In the coming decade we will see these threats expand, beginning to move into the social media domain. This will allow attackers to micro-target individuals for not only criminal activities but also as a means of influence and destabilization.

Cyber Physical Threat

Beyond the cyber to social activities, we see the attack plain moving into the physical world as well. To date most of these attacks have been comprehended as "go dark" attacks. This is when an attacker "takes down" a specific physical infrastructure like a power grid or security system.

Cyber Kinetic Threat

With the rise of complex automated systems, the impact of these cyber physical attacks become far more dangerous. A cyber physical attack could manipulate a physical system to take action. This action could be the attack itself or it could create a weakness in the physical work that then allows the attacker to launch a second kinetic attack.

The widening attack plain attempts to describe this emerging landscape. As we look at the future of cyber threats we must look beyond the current digital attack surface and see a plain that is far wider and exposed. The nature of hacking and cyber itself will simply become

another tool or weapon that can be used alone or with more frequency as a blended attack. These blended attacks provide the most potential and complexity.

Threat Actors

The threat actors in this widening attack plain seem to have stabilized. They still include the following:

- Vandals
- Hacktivists
- Criminals
- Criminals (State Sponsored)
- Terrorists
- Terrorists (State Sponsored)
- Terrorists / Hacktivists
- State Actors
- *Corporate Espionage / Destabilization*

Technological, cultural and economic changes however mean that there actors can and will work together in dramatically different ways. The very notion of hacking itself as a position, trade or category begins to disappear. In this new future, everyone can hack. Hacking and the ability to plan and launch digital attacks will be as common as purchasing hardware, software or even apps over the internet. Very little technological expertise will be needed to launch an attack, lowering the bar for vandal and hacktivists but also increasing the problem of attribution and track backs.

A potentially dangerous area that is enabled by the use of AI (profiled below) is that now larger criminal and state actors have the ability to watch the digital or cyber plain for opportunistic vulnerabilities. By having the AI "watch the plain" means that these threat actors can remain aware and be notified when an unknowing third party (e.g. hacktivist) opens up a door, allowing the state or criminal actor to opportunistically take advantage of the momentary weakness.

Each of these threat actors will certainly play a role in the threat landscape of the future. From our threatcasting, we have categorized this new threat landscape into two threat areas and two action areas. The threat areas are described below as the "War on Reality" and "Efficiency is Easy to Hack". The action areas (described later in the report) are "The Need for Norms" and "Living in the New Reality".

War on Reality: The Weaponization of Data and AI

In the next ten years, we will see the weaponization of data itself; data used as a weapon to spoof, obfuscate or hijack systems. Increasingly, the systems that we have to process data/information (and turn those nuggets into insights to take action on) are becoming increasingly automated as we are using complex algorithms to sift through the massive amount of data. This will only continue.

This construction exposes a vulnerability that will allow attackers to use data as a weapon. Meaning that the integrity of the data that is gathered and fed into the algorithms often cannot be validated and yet the system will still take action on that data.

There are some simple examples of this that have already happened. On April 24, 2013 Bloomberg Reported "AP Twitter Account Hacked in Market-Moving Attack"

> *Hackers hijacked the Associated Press Twitter account yesterday, sending stock markets down 1 percent in a matter of seconds by posting a false claim of an attack on the White House.*
>
> *The Twitter message -- saying that President Barack Obama had been injured after his residence was bombed -- followed repeated attempts by hackers to gain access to AP reporters' passwords, the news agency said in a report. The AP restored the account this morning after it was suspended yesterday pending a security review.*
>
> *The Standard & Poor's 500 Index fell about 1 percent yesterday before quickly rebounding, briefly wiping out $136 billion in value. A separate Twitter account operated by the AP's corporate communications team followed up minutes later with its own message: "That is a bogus @AP tweet."*

This example shows the effect that data can have and how it can affect these complex systems. The weaponization of this data will mean that attackers can use misinformation, not only to increase the fog of war but to manipulate reality (or how the machines and algorithms perceive reality) and then reality is reflected back to us.

When we have more autonomous systems, these systems depend upon data to construct a model of the physical and real world. If this data is corrupted or deliberately manipulated - could mean that these highly automated and thinking systems are not living in the same reality as we are. The information into these systems can be altered, falsified, spoofed, and

manipulated to not only affect the system but weaken or destroy it as well. The greater use of autonomy also means that this weaponized data can quickly move effects from the digital or cyber domain to the physical or kinetic.

The weaponization of data or information is nothing new in warfighting but the increasingly span of data as an input to these autonomous systems as well as powerful AI allow for a greater effect and a wide use across the attack plain.

AI is in use today but future advances in both the hardware and the software will bring about a kind of industrial grade AI, that will bring it into more common uses. This of course provides both greater threats and opportunities.

In the future, AI will be the backbone and chief enabler of all complex autonomous systems, allowing them to operate and make decisions. But the weaponization of AI also means that AI can be used as a part of these blended attacks - spoofing, hijacking and destabilizing both digital and physical systems.

AI can also be used to monitor this expanded attack plain, looking for vulnerabilities and either prompting or taking autonomous action on its own. For example, an attack might take place by a third party. A hacktivist takes down a system as a form of protest. But then a state sponsored or criminal network using AI could identify this un-associated action as it opens a window or vulnerability that they want to exploit. In this way, a completely unrelated and unknowing actor could work to further the desired outcome of another party.

In this way, AI and these highly automated complex systems become a key component in these blended attacks because the actors on their own will not be able to monitor the entire attack plain

Efficiency is Easy to Hack: Vulnerabilities of Complex Automated Systems

The second threat area is a direct result of our desire to produce more and more efficient systems/processes. Coming technological advances in shrinking the physical size of computational power, expansion of sensor networks, rising automation (on land, sea, and air), expanding smart cities and intelligent environments, the industrial use of big data and data analytics and the normalization of the Internet of Things (IoT) as well as the industrial Internet

of Things (iIoT) provides the ability for businesses and the global supply chain to undertake a massive wave of automation.

This automation and the use of sentient tools will bring about a large destabilization in the global workforce, increasing dissent, uncertainty and inequities sowing greater seeds of discontent. But it will also considerably widen the attack plain because these complex automated systems become high value targets for economic destabilization as well as physical and kinetic attacks.

Currently, there are very little regulations around the use of AI and automation. Globally, there is not a norm or accepted practice for human oversight of these systems or how the "human remains in or on the loop."

Our threatcasting revealed that the vulnerability of these systems is the very thing that will give rise to them in the first place: efficiency. Market forces and business management reward efficiency, whether this is cutting costs or increasing production; efficiency and productivity is valued over all things.

But as these systems undergo a wave of massive automation with the driving factor being efficiency, it means that for threat actors these systems become increasingly easy to attack. Stated simply: Efficiency is easy to hack.

If the threat actor knows how the system is constructed, what it values and how it has been optimized, then this threat actor can use both the weaponization of data and the use of AI to hijack and even use these systems as a part of the attack.

This vulnerability is increased because of the economic and cultural bias that business and specifically Silicon Valley have toward efficiency. Internally, management and executives are typically financially rewarded for increasing efficiency and productivity normally by cutting costs and labor. Externally, large and startup businesses alike are rewarded by the stock market and venture capitalists for shipping product above all else.

These realities, when paired with increased automation, highlight a wide area of vulnerability. This was highlighted several times as a key threat in our models of the future. Additionally, these systems are designed with security as an afterthought. Important to note, many systems are designed with a clear lack of understanding of the critical nature of these technologies when it comes to the welfare and security of the country. In fact, many of these systems have not been designated as "critical systems". This means that they have not been treated with the

same severity and precautions for redundancy and security as other similar systems like the energy grid or water systems.

To give more details and specificity for how the widening attack plain could be hacked, we have outlined three possible futures in the next section. These are based on the multiple threatcasting models generated at West Point. (See Appendix.) They are included here to provide us the detail we need in order to talk about what steps can be taken to avoid these possible futures. The other futures created and explored during the threatcasting workshop are included in the Appendix.

Possible Futures

The following three futures are pulled from the threatcasting models developed over the two day workshop at West Point. They give us a very real vision for possible threats and in their detail we can discover how to disrupt, mitigate and recover from them. The workshop produced fourteen futures. (The raw data for these futures can be found in the appendix.)

A Case of Misbehaving Appliances

The year is 2025, and automation is pervasive. From clothing to appliances to self-driving vehicles, it seems there is an embedded computer everywhere. The benefits of the Internet of Everything are taken for granted by most, but not all. Mike is a frontline supply chain supervisor working at a regional distribution center near the port of Red Hook, Brooklyn. On a crisp autumn day like today, he would normally kill time at work by tracking the value fluctuations of the handful of stocks he owned. The artificial intelligence running the complex logistics apparatus makes for pretty boring days, but not today.

The systems are struggling to keep up with a sudden uptick in demand for perishable goods. It seems to Mike as if everyone in the greater New York metropolitan area ran out of milk at the exact same time. As the smart refrigerators drive a surge in requests for perishable goods, the supply chain systems automatically expand their search area and start reassigning trucks to bring in supplies from further away to meet the demand. Routine items, like repair parts, are temporarily deprioritized to maximize profits from this unusual event. It would all seem great, except for the nagging feeling in Mike that something is not right. Autonomous trucks, even if they are commonplace in 2025, are still expensive assets that are never kept idle. If all the trucks are busy transporting this insane amount of groceries, what are they leaving by the wayside?

Mike is in the middle of running diagnostics and projections with this team when an unusual item catches his attention on his newsfeed. It seems that there is some sort of a hold up at the port and that the backlog of containers is getting way out of hand. The news mention something about inoperative scanners slowing offloading down to a trickle. Normally, all containers at the port are inspected by scanners that test for nuclear hazards before they can proceed. With multiple scanners down, the port authorities have to switch to random manual inspections of only a fraction of the containers. There is no choice. The problem is immediately obvious to Mike: with the sudden surge in demand for perishables, the needed replacement

parts, with their lower urgency of handling, will be held up somewhere in a distribution warehouse. Mike shakes his head, shrugs and goes back to the task at hand.

It is one of the last tasks that Mike will perform. A few hours later, an uninspected container arriving from Kraznovia and loaded with a combination of high explosives and radioactive materials detonates prematurely within a mile of his workplace. The massive dirty bomb misses its target of several million people in the heart of the city, but causes mass casualties, including Mike, near the port. Shortly before succumbing to radiation poisoning, Mike is able to connect the dots and realizes that the uptick in milk shipments was meant to delay repairs to the scanners and facilitate the delivery of the bomb. For the last time, Mike shakes his head and shrugs.

Reconnaissance

· The (fictitious) Republic of Kraznovia is an economic trade partner with the US, but an adversary in virtually every other sense, including sponsoring terrorism.
· A terrorist organization sponsored by Kraznovia has been conducting discreet tests of the ports' detection mechanisms for years. They notice critical failures in the gaseous ionization detectors that seem most frequent when ambient temperatures oscillate around the freezing point. Pretending to be news reporters, they offer to pay a port worker for notification of the next failure.
· The terrorists penetrate the vast supply chain system through a weak link owned by a small business in New Jersey. Through a read-only compromise, they can watch (but not alter) the flow of millions of items through the region.
· The Kraznovian-sponsored terrorists hire the services of a darknet crime-as-a-service provider to access a botnet consisting of millions of smart refrigerators in the New York City area. Despite calls for increased security, these devices remain vulnerable to sophisticated attackers.

Execution

· The port employee calls the fake news reporters late on the day before the attack to describe how not one but two of the three scanners had gone down the night before.
· The terrorists pinpoint the location of the spare gaseous ionization detectors within the supply chain. They are sitting at a distribution center in Pennsylvania awaiting shipment. Unless a higher priority item bumps them, they will be shipped within a few hours.

· The refrigerator botnet springs to life, directing every appliance to order large quantities of perishable dairy products for express shipment at premium rates. This surge fools the intelligent supply chain systems into maximizing profits by delaying other shipments.
· The detectors remain sitting in Pennsylvania, though the port personnel are unable to ascertain their exact status. After hours of impasse, this prompts the decision to go to the manual backup mode of inspecting containers, giving the terrorists a 90% chance of getting the bomb through.

Aftermath

· The loss of life, while not as high as it could've been, is severe.
· The complexity of the attack, together with its use of multiple proxies, makes attribution difficult.
· The attack prompts the government to regulate standards of security for supply chain operations, but, sadly, is not enough to prompt systemic, meaningful changes to security for appliances and other Internet of Things (IoT) devices.

Medical Device Take Over

- Nurse Jackie lives in San Francisco and has devoted most of her life to helping people. She started life as a nurse and had a revolutionary idea on how to make patient care better but limited tech skills. Jackie created a company and is the CEO.
    - She has 100+ people working for her now. They developed tech and software to "read human minds" to get a better handle on pain and physiology affecting the patients in order to provide better care.
    - They can then use a combination of drugs and modification of brain patterns/waves to eliminate pain.
    - Now that they have figured out a way to effectively remove pain, other foreign actors want this tech to enslave their dissidents.
- Their latest product is an in-home robot. The idea took off so well that many hospitals are also use this technology, abandoning some of their traditional ways to do pain management.
- Then...Jackie sees newspaper reports about her robots malfunctioning and medically disabling the patients by turning up the pain (vice turning it down).
- She starts to receive complaints by loved ones of individuals using robots. There are also news stories from this group (while not claiming responsibility) - they are spinning about how this is bad and proves their point.
- There are lots of OpEds. No explanation on why this is occurring.
- Jackie is frantically calling her technical staff together to begin analysis on what is going on.
- FDA gets involved.
- The scene is frantic as human's lives are being affected...
    - Multiple news stories with old folks and children in pain being shown.
    - There is such a pervasiveness of this technology that they are not initially sure how to re-call or roll back. What they don't see or understand initially - is where this all happened, what caused it ... what is malicious (software or hardware).
- No one thought that someone was taking over the robots
    - it was first assumed that the robots were the malicious actor ... based on what the spin in the media and this group was doing.
- To fix the problem...The FDA strongly recommends shutting off the robots but the issue is that the hospitals are not able to cover down on the medical requirements because they have also switched to robots to handle pain management.
- There are not adequate supplies of drugs or trained personnel to handle the need for pain management in the city.

- There is a panic. The governor calls for state of emergency as these robots are not just used in San Francisco but also throughout the major metro areas in the state.
- Nurse Jackie reaches out to FBI Cyber Division to assist with the analysis on what is causing it.
- They ultimately determine it was an issue embedded in the second generation chipset that is manufactured in a foreign country.
- Other government agencies reach out to assist with determining feasible solutions to fix. The hardware was subverted ... the actual code and communication with the devices was secure.

A Blended Attack

The Summer Olympics, also known as Games of the XXXIV Olympiad are to be held in Los Angeles, California. It's been over thirty years since the Summer Olympics were last hosted in the United States. Without surprise, societal reliance on technology has continued to increase in all aspects of everyday life.

Our story revolves around Logan McGuffin who is a well-respected and hardworking pharmaceutical sales man. Recent advances within the medical community and with medical bio-technology, have caused a huge boom to pharmaceutical sales. Logan has a family of three, including his wife. Both him, his wife, and two college daughters have that latest models in self-driving cars.

Logan spends a lot of time on the road visiting new clients and working to sell his portfolio of products. He is not a Los Angeles native and hates traffic. Traffic has become even worse with the Olympics in town. Thankfully, Logan's self-driving car saves him a lot of time on the road and has stored all of the addresses of the places he visits for convenience. Even with traffic, his vehicle is able to download traffic patterns and to automatically adjust routes and arrival times within seconds of accuracy.

One day while out and about, Logan's car can't find his client's location. He confirms that address and location are inputted correctly but still has no success. As a backup, he opens up his smart phone to access his mapping application and gets a similar result in that location services are not functioning. Logan tries to call out using his cell phone and there is no signal either. His entire day is disrupted. Being in an unfamiliar part of the city, he struggles finding his way home and then gets stuck in traffic. What a way to end a day.

Unknown to Logan and millions of other frustrated Americans, is that their lack of access is a result of an attack on key internet infrastructure routers across the US. The digital attack involved malware that caused physical damage to key devices requiring onsite replacement of hardware. Internet across the US is severely degraded with unreliable estimates of repair times. The effects are so widespread that both commercial and government entities scramble to resolve and restore normalcy.

News, public, government, and military functions are impacted to varying degrees. Air travel is disrupted and halted in many locations. Supply chains are impacted as UPS, FEDEX, and US Postal are crippled due to their reliance on routing schemes and navigation dependencies.

All of this happens during day three of the Olympics. Simultaneously there are 3 effective bomb attacks across the city of Los Angeles which are coordinated through a non-state actor terrorist organization. This organization is the same who launched the internet attack on US infrastructure routers. The attackers want to hurt the US economically and morally through causing chaos and disorder by disrupting the Olympics. The Olympics is targeted because of the great international symbol it poses and because of the strong presence of international leaders at the various events. The terrorists' goal is to instill fear in both Americans and participating countries. Several weeks later, investigations show that the attackers were radicalized within the US and are all US citizens.

Clusters

During the threatcasting workshop, participants created fourteen different futures in which a person was in a place doing a thing. However, further analysis showed that there were common themes within these futures. Using a clustering process on the futures allows us to examine, in detail, all of the threats and actions that need to be taken in the future scenarios and look for patterns. These patterns give us a way to process the next steps we might take to disrupt, mitigate and recover from the threats.

At the end of the threatcasting workshop, we engaged in a clustering exercise. The collection of threats and actions could be categorized into these four distinct areas: War on Reality, Need for Norms, Efficiency is Easy to Hack, and Living in the New Reality. Two of these are threat areas while two are areas for action.

The data below is a collection and curation of all the threats and actions identified, with details and specifics. These clusters form the basis for our previously discussed findings and many of the clusters below reference specific raw data and worksheets from the event. These specifics can be found in the Appendix.

Threat: War on Reality - The Weaponization of Data

- Reality management (reality assessment) is critical as many physical/life-death decisions hinge on determining what is real and legitimate. Automation and virtualization can inflate, obscure, and alter reality.
- Behavior modification through misinformation. Systems engineering: intentional delay based on lack of feedback. Exploiting the gap in information - the gap between real and synthetic reality. Explore a mechanism to analyze decisional data faster and validate the reality.
- Trust in the system. At what point on the spectrum from real to synthetic is the tipping point where we lose trust in the system? How do we correct the margin of error? If I defer to the machine am I protected/rewarded/wrong?
- Open source big data pulls introduce many points for misinformation. Aggregating many "false positives" through data feeds can severely disrupt larger systems which are implementing this information without secondary checks.

- Data Ownership. Ubiquitous cloud-based storage of all data by third-parties has vast implications on privacy, anonymity, and vulnerabilities. Individuals can't opt out in the future. Additionally, if information from our home devices are collected and stored by third-parties, does it still maintain its protections under the 4th amendment as part of the home?
- Data storage and ownership. Who owns what? When do we give up our right to the information and to its protection?
    - *Threatcasting Example: Social Panda, Health Club Fiasco, and perhaps was so obvious that many of us did not put into our futures. It will still be an issue 10 years from now ... especially as you add in the idea of PII and what is the next evolution of PII.*

Threat: Efficiency is Easy to Hack: Vulnerabilities of Complex Automated Systems

- Human in the loop. With the increase in technology and eventual passing of the Singularity Point, we cede more functions to autonomous machines. What skills do we need to retain proficiency in? For what things do we need to stay in the loop over? How do we query machines to explain their decisions if it does not make sense to the human? So, you need to design machines that have a place for humans that can "dumb down" the machines decisionmaking so that it can be explained to humans, or "smarten up" humans to understand the machine. Ultimately, must also think about what skills/capabilities that humans need to maintain in case all the machines go dark. This was seen in:
    - *Threatcasting Worksheets: Robot Pain Train, Here Comes the Hammer, Detroit X, Logan Has a Bad Day LA*
- Increasing use cases for automation and technology to replace tasks performed by people.
- The need for new technology which facilitates secure communications between parties.
- Hardening of the internet ... and other mission critical utilities. How do we do this? As we rely more and more on these systems in our daily lives, we must develop ways to harden the infrastructure for everyone’s use.
- Cyber resilience of systems and self-diagnosis/validation.
- Automation Backdoor Access - building in fail safes for the automated systems we have created to allow humans back in.
- CRISPR for code - modifying code to shift intent or application of technology rather than changing the core of the technology itself.

- Increasing use cases for automation and technology to replace tasks performed by people.

Action: The Need for Norms

- Rules. There is a need for international norms and rules (irrespective of cultural or social rules/norms) for the cyber domain. Technology is designed to integrate across the realm and is not constrained by physical boundaries (i.e. Nations, societies, cultures). Therefore, an international consensus is required to develop both rules to deal with “bad guys” and minimum standards for cybersecurity in tech. These are seen in most scenarios, but specifically in:
    - *Threatcasting Worksheets: Health Club Fiasco, Heart of the Sea, Project Mayhem, Infernal Combustion, etc.*
- The need for adopting standards across policy, security, technology, and safety. A holistic approach/view is needed taking into consideration both the technology itself and its proposed uses.
- Unclear cyber boundaries. Ethics, behaviors, expectations, and legislation need greater definition in order to govern national and international relationships.
- Integration of tech advancements in an “cybersecurity ignorant" society creates social tension and potential harm. This could artificially create a caste society (haves / have nots).

Action: Living in the New Reality

- Emergence of diverse future adversaries both in how we think of who they are and how they will operate. In general, it will get progressively harder to determine intent from actions as the action surface increases as well as available technology/skills. This was seen in:
    - *Threatcasting Worksheets: Robot Pain Train, Health Club Fiasco*
- Impact of ever-changing societal/ethical norms; ex. kids today believe that grabbing digital content without paying is okay but still think that taking a candy bar from a store is not ok. Therefore, we are entering an age where actions in different domains have different right/wrong values.

    - *Threatcasting Worksheets: This was seen in: Rise of the Social Panda, Health Club Fiasco, Infernal Combustion, the Fall of the Machines, Group 4's un-named scenario from Day 1.*
- With the global nature of the cyber domain, you might be talking to someone that is from a different cultural norm/background ... that is also a concern. The problem is the anonymity of online actions and the belief that they won't get in trouble.
- Indirect attack vectors that adversaries are using. For instance, they are not attacking the credit card directly, but also the refrigerator to get to the same place. This was seen in:
    - Threatcasting Worksheets: Logan has a bad day in LA, Code Red, Project Mayhem
- Micro targeting. The use of micro targeting that is both bad and good.
- Increasing social acceptance of giving up personal privacy for convenience or safety.
- Known and predictable human behaviors and interests still "drive the train" despite being sometimes obscured by technology.
- Hacking (such as intrusions, exploits, etc) will always happen and will scale linearly in the future. These cannot/will not be eradicated. Our futures see that the levels of attack and ability to defend will stay at their current balance (but is this a good assumption).
- Transparency to allow grassroots decisions. Not transparency over a global system, but across the local systems in use. Generating a global system creates a single point of failure. There is an advantage to creating a decentralized system (opposite of TPP).
- Behavior, political, and tactical changes start virally and disseminate outward, rather than taking a top down strategic plan approach. Note: routinely seen that many management layers of organizations are not ready to tackle strategic changes in this space.

A Widening Attack Plain - A Threatcasting Framework

A Note on the Threatcasting Frameworks

In threatcasting, frameworks are used to gather together and organize the large amount of data we produce. They provide us a way to dig even deeper and process new information. They are the tools used to measure, evaluate and take action.

The following is a step-by-step explanation of the framework "A Widening Attack Plain" and how it can be applied to the future activities of the Army. It combines the previously presented information in this report to visually describe the attack plain in 2026.

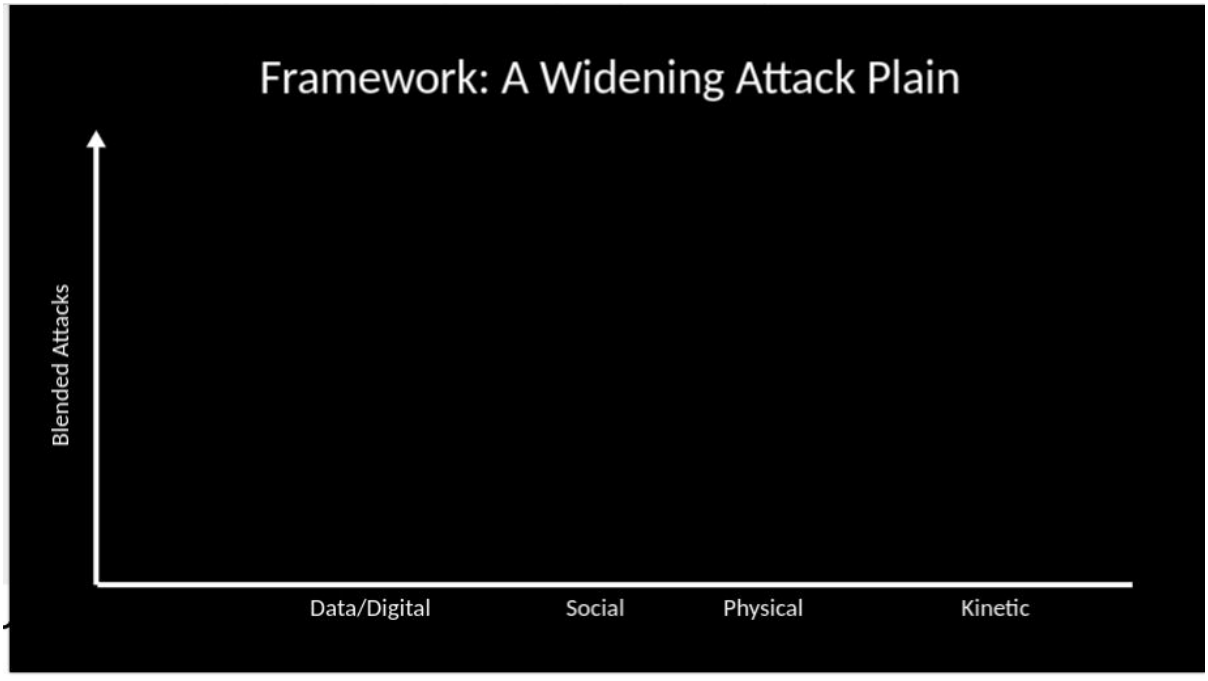

Figure 2: A Widening Attack Plain Framework Construct

The coming technological, economic and cultural changes show us that the attack plain for cyber and digital threats is widening. We will move from digital only threats to cyber-social to cyber-physical and finally to cyber kinetic.

Additionally we see that the threat actors will take advantage of this widening attack plain by participating in blended attacks, these are attacks that might start off in the cyber (data) domain but will spread into the other social, physical and kinetic areas.

Some future models show that the notion of a cyber only attack or a simple cyber attack could become a simple weapon attainable to not only current threat actors but the general public as well.

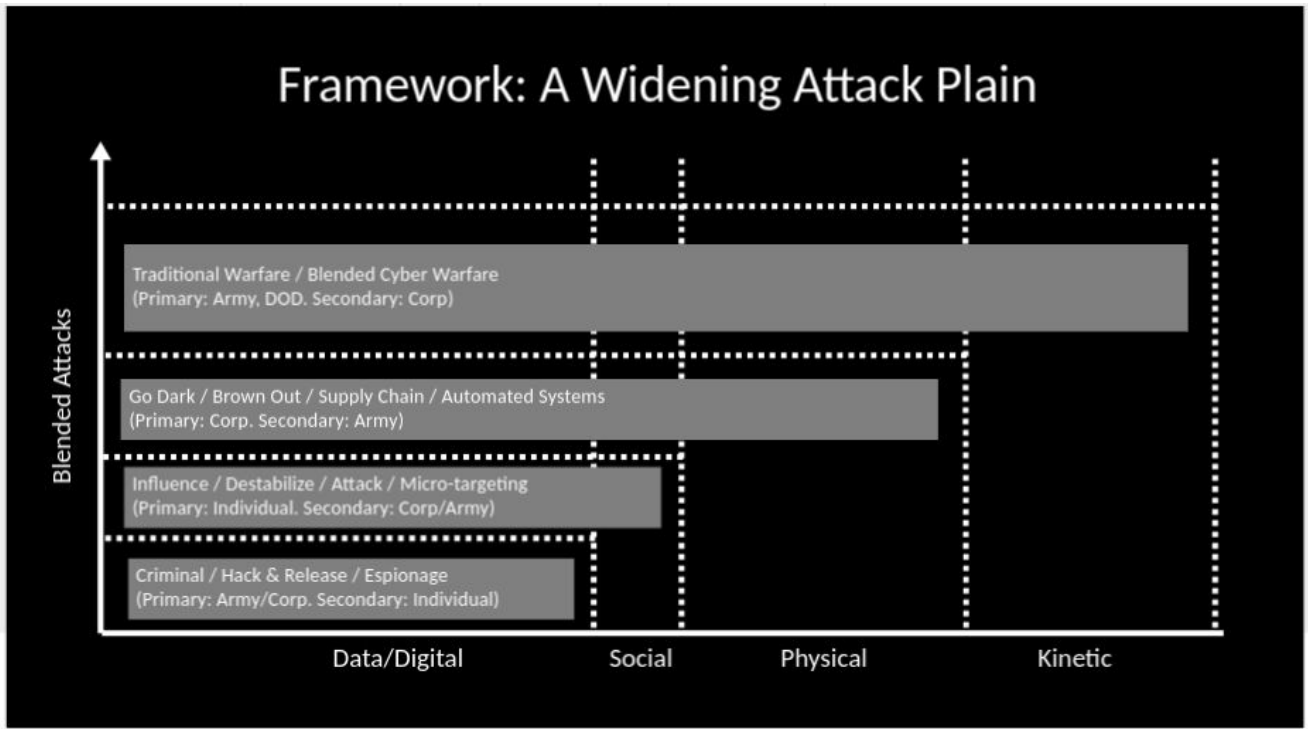

Figure 3: Mapping of multiple blended attacks with overlay of lead defensive actors

By mapping the attack plain in this way, it allows us to understand not only the implications of each of the areas but who are the participants (e.g. Army, DoD, corporations, individuals) who will both be affected and/or called upon to take action. Figure 3 visually describes the classes of blended attacks and whom the primary and secondary actors could be.

Data/Digital

This more traditional area for cyber attacks will continue to see criminal activity, hack and release operations, traditional espionage and IP theft. This is a traditional area for the Army

and the DoD to operate within and will continue in the future. However, the space becomes more crowded as corporations strive to protect themselves and their products.

Social

The social attack or cyber social attack is one of the more problematic emerging areas of the attack plain. Here, attackers micro-target a single individual or group of individuals to attempt to influence or destabilize the person's life, economic standing, family or broader social network. When paired with the expansive power of data and AI as a weapon, the subtlety and sophistication of this kind of attack is great.

Even more troubling about this area is that the Army and the DoD have very little role to play. In fact, there are many areas of this where it would be inappropriate to take action. One area that could be considered as actionable would be when this type of attack involved a Soldier or a Soldier's family. Again, with the weaponization of data and AI this type of attack could happen on a massive and/or micro-targeted scale.

For the general public, the Army and DoD would need to act as a trusted voice, possibly talking about the potential threats and what both individuals and private industry can do to protect themselves. By strengthening the individual, it reduces the attack surface of this portion plain.

Physical

Cyber physical threats have already begun (such as power grid and water system hacks) but with the technological progression discussed previously that will be realized in 2026, this area increased its vulnerability with highly complex automated systems becoming the prevalent.

Here, there is also a limited amount of work that can be done by the Army and the DoD. Most of the responsibility for protecting this part of the plain will lie with corporations, local government and private industry.

There is a dual approach that could be appropriate. First, we can rethink what it means for a system to be a critical systems - that is a system that is critical to the economic stability and security of the nation. This would then put a different level of requirement on the companies that want to design, build and profit from these systems.

Secondly, the Army and DoD can collaborate with appropriate entities to establish New Norms for what it means to develop these types of systems. Meaning that it could become an enabler for technological training, a convener for industry, and a trusted ally for the protection of these systems even when they are not deemed critical. Finally, the Army would need to maintain situational awareness of this space in case ever called to conduct offensive operations on similar infrastructure abroad or to assist with the defense of our nation's infrastructure.

Kinetic

The kinetic area of the plain is the most traditional space for the Army and the DoD. This will only continue. But with its place as a trusted ally and convener, the corporate and private industry ties could help make the actions in this area more effective.

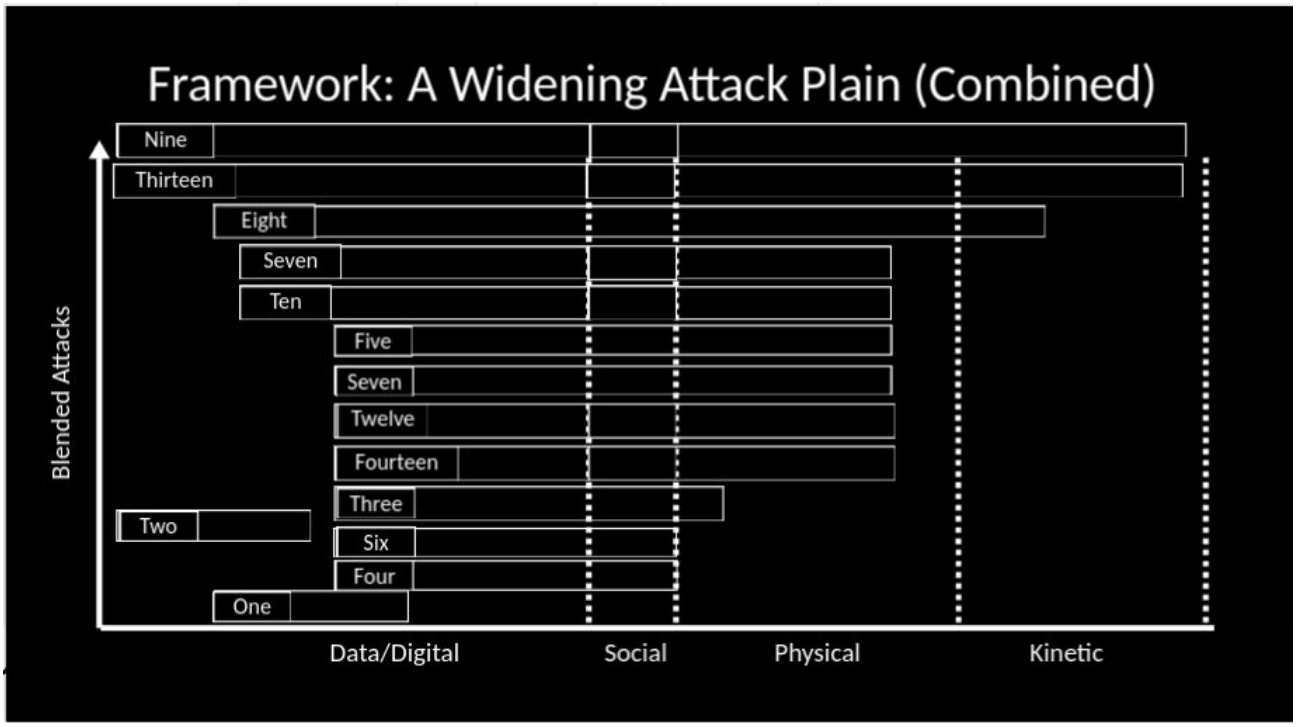

Figure 4: Mapping of the Fourteen Futures across the Attack Plain

The visual above (Figure 4) shows how each of the fourteen futures developed at West Point overlay on the widening attack plain. They show the growing nature of blended attacked and

also who will need to be involved in their disruption, mitigation and recovery from these attacks.

Here, it becomes clear that the Army and the DoD's role is a once both large and small in the coming threat landscape. These blended attacks mean that the Army needs to be more nimble and better networked in places where it typically has not played in the past. This will place more stress on the traditional areas of the organization, pushing it to make changes that will receive considerable push back as any large organization feels when implementing cultural change.

Analysis

Threats and Actions Identified

For us to begin outlining next steps for the Army we must first identify both the high level threats identified by the threatcasting session as well as the potential next steps for actions.

Using the clustering and the Widening attack plain framework, we can identify high level, aggregated areas of threat and action. In this landscape of complex global autonomous systems, AI and the reality of an insecure supply chain we have identified clusters of threats and needed areas of action over the next ten years:

- Threat: War on Reality: The Weaponization of Data and AI
- Threat: Efficiency is Easy to Hack: Vulnerabilities of Complex Automated Systems
- Action: The Need for Norms
- Action: Living in the New Reality

The widening attack plain presents an expanded set of possible threats but also opportunities as well. Additionally, because the attack surface is so wide it will mean that individuals, industry, educational institutions and many more public and private participants will need to be involved. In fact, there are wide swaths of the plain that cannot be defended by the Army or the DoD.

In this new landscape, there will be greater pressure and responsibility placed upon these new participants. This will facilitate the need for guidance and new norms around security.

The widening Attack Plain framework is a way to illuminate these new relationships and responsibilities to these new participants. (See Frameworks.) The informing, training, coordination, collaboration and influence of all these new participants will be the biggest tasks, far greater than simply the cyber security functions alone. A new AD HOC network of information and norms will be needed, with increased public, private, academic and general public relations.

In fact, the Army can take an active role in this area to provide much needed guidance and training that enables these new participants to take actions. But the Army itself will not need to take the action.

The following outlines specific actions (gates) and details that the Army can engage in as well as the specific external events (flags) that needed to be watched and monitored. This is not an exhaustive list, but it begins the process of defining specific areas for investigation and action by academia, government, military, and private industry.

Potential Actions (Gates in Detail)

Broadly, the gates are actions that the Army can take to help disrupt, mitigate and recover from the future threats we have described. The participants in the August threatcasting workshop used a backcasting process once the futures were described (see bottom of Figure 1). They focused on the threat to a person in a place doing a thing that they described in their future. Then they explored how to disrupt, mitigate and recover from this threat - understanding that if we need to be successful in 2026 against the threat, then we need to start today to lay the needed groundwork.

The gates on the paths to our fourteen futures are diverse but they fall into three aggregate categories (with respect to what the Army can contribute): Army specific actions, Army collaboration and Army influence.

The Army direct actions will be the easiest to enact. They are described as specific actions that fall within or close to the charter of the organization. The collaborations and influence categories will be harder to bring about because they involve working in a highly complex and diverse ecosystem of public and private organizations. Because of this, more effort may be needed to further the latter two gates and less attention placed on the Army direct actions.

The following gates (actions) were provided/suggested by the threatcasting participants to influence the fourteen created futures:

Army Direct Actions

- Sponsor research in the exploration of future attack vectors against society. As the population ages, utilize understandable cues people have on technology and how this influences people's ability to recognize if they have been micro-targeted.
    - What are the things that will target our generation?

        - Community experiment (perhaps using crowdsourcing techniques) with the Army Cyber Institute (ACI) as a sponsor
    - Explore the *what if game* (on possible attacks as our generation ages)
    - Determine generational blind-spots

- Use ACI events as platforms to champion the threats that have been identified
    - Promote these goals and help find military, industry, academia and general public that want to research these ideas to solve these challenges.
    - ACI to target outreach and events to collaborate and influence

- Build relationships between influential industry and academia leaders with key Army leadership in order for the Army forces to become recognized as a credible source for cyber expertise.

- Focus on a standard for end-to-end encryption to protect critical infrastructure, especially in the future IoT scenarios with increased automation. Through the use of these techniques in Army systems, demonstrate benefits to other critical infrastructure activities.

- Shore up and strengthen physical face to face bonds and interactions among people living in physical communities and work areas. Create a backup social construct that will endure after a Cyber 9/11 event and be resistant to cyber hacking.
    - Army focuses on implementing construct amongst its forces and then export the ideas to society-at-large.

Army Collaboration Actions

- Champion a national cyber threat sharing center with established rules that could potentially imitate the ISAC construct. However, it adds the ability for the general public, corporations and academia to report as well.
    - Possible current gap in over-arching on all the current ISACs
        - Need a way for multiple parties to contribute and report
            - Information gathered can be seen by other contributors and individuals or organizations.
            - Must be overseen by a trusted entity.
    - Essentially create a “community bulletin board for cyber"

- Promote broader cross collaboration with multiple agencies and organizations.
    - Data sharing allows for comparisons for similarity, repetition, and duplication.

- NIST/SISO Truth System. Collaborate with academia and industry to develop a vetted, democratically backed, secure, transparent "black box" fact checker that uses AI to score knowledge/data/information as to its probability of being true. Controlled and owned by the people.
    - Manage design and tuning so that it stays as objective as possible. This is information assurance, but needs to be global, real time in some cases.

- Advocate for international standards for automation and human control.
    - Develop metrics (via organizational psychology and systems engineering) to test and understand the correct level of human control and redundancy.

- Develop guidelines and/or recommend policy to help shape acceptable tasks which should be automated and what safety measures are applicable; consider interoperability amongst services.
    - Act as a trusted and credible source.
    - Advocate for increased interoperability amongst the branches of military service with respect to technology.

- ACI (and other Army research entities) should collaborate and help shape trade associations, industry collectives and groups' (e.g. IEEE, ISACA, APICS, etc) strategic plans for cyber and hardware security/transparency standards.

Army Influence Actions

- Develop/influence the behavior of nations as part of a whole-of-government approach. Help start the conversation on international norms. (e.g. UN, NATO, etc.)
    - Is it possible to develop what rules should be?
    - Advocate for all the countries and organizations to collaborate and "play nice with each other"

- Develop/influence the behavior of individuals as they operate within the cyber domain.
    - The Army has a problem with how Soldiers use social media or respond to phishing emails (links) and we are attempting to combat this through education.

    - ACI can help the Army open the aperture of this so that we are not responding only to current threats but educating on the future and its rapid change.
        - Explore ethical right/wrong rules in the cyber domain that new recruits are going to come in with.
            - How do we modify this behavior in individuals?
            - How do we change the Army ethic to include this?
        - Possible starting point for this education could be at Army intake of members but should grow/be exportable to share across society.
            - How do we "teach everyone to be responsible cyber citizens”?
            - Could a public service announcement campaign (similar to the 1980’s “This is your brain on drugs” campaign) work?
    - Educate service members and the general public on the consequences of actions in cyber domain with focus on negative.
    - Explore cultural norms around behavior in cyber domain.

- Encourage research in the decision making process of AI and machine learning, and ultimately turn that into output that is human recognizable.
    - Can AI become intractable to use?
    - "teach machines to play nice with us"

- Promote education of future generations to better understand security implications of privacy.
    - Sponsor an open call to develop educational ideas on how to influence STEM education in K-12 throughout the nation in order to create a more technical future workforce that can compete with other nations.

- Advocate and educate for policy purposes
    - Goal: working with people who already agree with general goals, but who have the ability the make change (e.g., trade groups, academia, corporations)

Indicators and Events (Flags)

Also found during the backcasting process are flags. Flags are events that are key steps, advances or indicators that the possible described futures are moving toward the conditions that will help bring about the threat. These are typically events that an organization cannot control. Also when a particular pre-identified flag occurs usually there is no going back from the event. Types of broad flags could be technological developments, natural disasters, economic or political catastrophe but once the event has occurred, there is no going back; the event cannot be undone.

By monitoring identified flags, organizations and teams can prepare for possible futures and have a plan for them when they do happen. These flags also mark specific progress along the ten year time line. If an expected flag has not happened then it could be an indicator that there is something amiss in the possible future and it might need to be reconsidered. This could be due to a shift in the inputs or new data points (recall the curated technological, cultural, and business trends that focused the threatcasting session). This new data could alter slightly the futures that were modeled, pushing them out further into the future or altering them to the point that the flag is no longer relevant.

The collected and aggregated flags from the West Point Threatcasting Workshop have been placed into three distinct areas: technological advances, hacks and attacks, and cultural and societal changes. The technological advances are the enablers of the various threats. They do not create the threats but they provide the attackers with the tools they need. The hacks and attacks are evidence that we are moving toward a specific kind of future. Each hack and attack that happens is an indication of the progress in the widening attack plain. Finally, the cultural and societal changes are the indicators that the broader public is changing, with new outlooks that can help to prevent or enable cyber threats.

By constantly monitoring and sensing, we can use these aggregated flags as indicators on our progression toward different kinds of threats. They can also serve as specific signs that more immediate actions need to be taken. If they do not happen, then conversely it could show that the threat or the conditions needed for the threat are yet to happen or might not ever materialize.

Flags: Technological Advances

- Robots and drones are used to autonomously kill in both war (by military forces) and in domestic scenarios (be law enforcement).
    - The use of drones to kill on the battlefield has been occurring for a few years, it only recently occurred in a domestic situation. However, these can be considered as just a long trigger over a wireless connection as humans still make decision to shoot.
    - "Police used a robot to kill -- The key questions" Peter W. Singer Sun July 10, 2016.
        - *"The use of a robot to kill the man who authorities say fatally shot five Dallas police officers has drawn attention in part because it's the first time police have used robots in such a manner."* http://www.cnn.com/2016/07/09/opinions/dallas-robot-questions-singer/
    - The next iteration of this gate would be for AI or semi-autonomous systems to kill. This would continue our society along the sliding slope to full autonomy.
    - Then we would arrive at a technological advance of a complete autonomous system killing and society's acceptance of it first in the context of military operations abroad and then by domestic law enforcement within the borders of the United States.
- Major advance in automation that enables automation to self-organize, self-maintain at a level that makes human oversight irrelevant and/or cost prohibitive.
    - Follow up - watch for insurmountable pressure (economic, technology) to get the human out of the loop.
- Proliferation of disposable, cheap tracking (wearables) devices.
    - Where the proliferation of information about the individual via their wearables or others' wearables create a situation that you can no longer opt out of being tracked.
    - When micro-targeting of individuals become commonplace and un-stoppable.
    - Society re-thinks what the concept of privacy really looks like given the technological advances.

Flags: Hacks and Attacks

- Election hack or information hack around the election that causes people to question legitimacy or cause loss of international prestige
    - "US gives detailed look at Russia's alleged election hacking" - TAMI ABDOLLAH, ASSOCIATED PRESS WASHINGTON — Dec 30, 2016 http://abcnews.go.com/Technology/wireStory/us-detailed-russias-alleged-election-hacking-44465995
- "Cyber 9-11" or media equivalent

- Automated vehicle hack resulting in:
    - loss of life
    - significant financial compensation
- Amazon supply chain hacked
- Major cyber-enabled corporation experiences a substantial blow to their bottom-line from hack or intervention
- Pokemon Go hacked
    - Gamers information and lifestyles documented, used to predicted with a higher degree of resolution activities
- Massive data breach tied to an experience or specific location which is immediately felt, pervasively catastrophic and changes behavior of those affected ~150k members
    - e.g. bank accounts wiped for everyone in NYC
- A benign product is hacked and used for malignant purposes
- United States actually responds to a cyber attack with a physical (kinetic) force/attacks and acknowledges it in the public domain
    - National policy allows for this action however, if we did respond with a kinetic attack it would indicate that we have lost supremacy in the cyber domain as our only response option left to stop a digital attack would be to kill people
    - Indicates that someone has outpaced the rest of the world with their capabilities in the cyber domain, then we would expect that all future responses would be asymmetric in nature

Flags: Cultural and Societal Changes

- Abolition of European Union privacy laws result from either legal battles or (worse case) the collapse of the EU.
- Global Recession
- United States renounces NATO membership
- United States cancels trade agreements with NAFTA, TPP
- Reversal of net neutrality policy which loses the “openness” of the Internet
- Tipping point: geographic communities and local relationships are non-existent; majority of influential, accepted, and "trusted" social communities are 100% virtual opening up larger attack plain with greater consequences
- Expansion of identity definition (e.g. gender to spectrum, splintering online identities, or multi-person shared identity)
- Economic sanction or legal conviction of a group identity, those in the group identity share responsibility

- Cybersecurity event trigger mass exodus from digital mainstay (e.g. Facebook, LinkedIn, SAP, etc)
- Society recognizes responsibility as shifting from the human (driver) to the machine (car) or cyber agent. Legal and regulatory shifts to manage risk and culpability
- Cyber as its own service. Army, Navy, and Air Force combine all cyber forces into a fifth military service representing an acknowledgment of the permanence of this new domain of war fighting.
- Internet Service Providers (ISPs) shift to becoming Information Service Providers by making choices on what data is provided/available to society

Milestones

Once the Army and DoD begin to enact elements of this plan for combatting the negative futures, taking the actions outlined in the gates as well as watching the external developments outlined in the flags there needs to be a way to measure success.

The following details provide specific targets that the Army can set to track its progress to this vision on both a 4 and 8 year timeline. These milestones were suggested by the threatcasting participants and cover the Army direct actions, collaboration actions, and influence actions. This underscores the concept that if we desire a change in vision of 2026, there are actions that need to be in place by 2024 and for those actions in 2024 to be successful, there are actions that we need to take by 2020. And if we want successful change in 2020, we must start today.

In the next 4 years...

- Identified and partnered with the appropriate stakeholders to affect our previously identified gates
- Develop threat sharing framework for the global community ISAC (bulletin board)
- Conclude pilot study on "Cyber Citizenship 1.0"
    - Explore previous mis-matches in society (e.g. slavery and equal rights)
    - Explore norms for medium vs. message - double standards: what is appropriate to send on telegraph, mail or telephone vs. in person.
    - Cultural history could give us new language to establish norms and language.
- Engage companies to explore where safety mechanisms should be in place
- Use lessons learned from High Frequency Trading / stock market crashes to apply to other sectors
- Conduct study to help identify previous breakdowns in complex systems (e.g. factories, trains, and subways) and apply to resilience of possible automated systems (e.g. supply chain, smart cities)
- Collaborate with industry organizations (e.g. IEEE, ISACA, APICS) to expand cybersecurity in specifications, policies and training
    - Publish standards and norms for hardware and cyber protocol
- Organize and promote cyber drills and pedestrian pen testing at the national level.
    - Promote cyber-readiness and resilience to reduce fear and induce trust in the system. (Previous example: national drills during the cold war)
        - Goal: reducing threats through changed behaviors

- Develop the set of international rules or norms (ala NIST) for big data privacy and big data use
    - Work with organizations to get policies and norms in place to establish appropriate level of human-in-the-loop interaction and need for local redundancies in political, economic, transportation, healthcare, military processes
        - Create a model that can do the following:
            - measure the ratio of automation/human redundancy in a given system (in a general sense that can be ported across many domains)
            - establish minimum acceptable ratios for various categories of systems.
            - Example: certain critical systems might require a minimum ratio of human redundancy
- Advocate, educate and enable encryption standard in IoT devices.
- Develop metric for measuring the ratio of virtual communities to local/physical community in a geographical area.
    - Example: if the people living in Hamilton, OH have 90% of their relations and social interaction with people outside Hamilton is this community resilient to hacking/Big Data manipulation?
        - How can governments, policy makers and community leaders alter this?
        - Develop a metric for understanding the problem is an important first step.
- Develop a set of third party norms that can be used by industry (e.g. app developers and companies) for the appropriate collection and handling of personal or sensitive data.
    - Apply to individuals, family members (children and elderly)
- Research and explore Identity tokenization for attribution of known personas
- Create data access notification system in order to see an overview of personal data and who has accessed it (e.g. credit score for data usage)
- Research and develop automated system prototype
    - Fail safe aspect includes humans in the loop with moderate monitoring by humans

In the next 8 years...

- Develop requirements, specifics for implementation for the global community ISAC (bulletin board)

- Gain from NGO or charitable foundation for continued cyber hygiene/citizenship development
    - Goal: Transfer and hand-off to another organization.
- Extend cyber drills to megacities. Go beyond army readiness to national readiness.
- Trade organizations (IEEE, ISACA, APICS, etc) have implemented standards and norms for hardware and cyber protocols
- Digital government approved identity system (virtual and physical identity integration)
- Creation of unified shared data stream for all government agencies

What's Next

The true power of the threatcasting process and the results that come from it are to provide organizations and teams with both broad futures and specific actions. For this to be truly successful, it must be used, implemented and iterated. It has been clearly shown that no single sector or element of society is solely responsible for nor capable of combating these negative futures. It will be a group effort that starts with collaborative research on the gates.

The ACI and the broader threatcasting team is reaching out to and collaborating with multiple domains (within the military, federal, corporate, academia, media sectors as well as general public) to apply these findings and discover areas for further investigation and modeling. Ultimately, to help others understand what they can do to help given their expertise and capabilities. In support of this, a Threatcasting Lab is being set up in 2017.

ASU Threatcasting Lab

Based at Arizona State University's Global Securities Initiative and in the School for the Future of Innovation in Society, the Threatcasting Lab will host and manage the Cyber Threatcasting Project. Over a five-year timeframe, the Threatcasting Project will conduct interdisciplinary, collaborative sessions twice a year to envision future cyber threats ten years in the future. Each session will alternate from the east (West Point, NY and Washington D.C.) to west coast of the United States (Tempe, AZ and San Francisco, CA) and will produce a threatcasting report like this one that explores specific aspects of cyber threats and cybersecurity. Each report will also contain specific actions, external indicators and milestones that can be taken to disrupt, mitigate and recover from the threats. These report will be shared between government, military, academic, public, private and corporate audiences.

Ultimately, we will bring together a diverse, interdisciplinary collection of people and organizations to model possible threats and specific actions that can be taken today. We will use the output to foster conversations and dialogue with a wide range of audiences (e.g. military, industry, academia, policy makers, trade associations, law enforcement, etc.) with a diverse set of deliverables (e.g. Threatcasting Reports, briefings, articles, podcasts, videos, science fiction, etc.).

We feel it is important to bring together a wide variety of people and organizations to not only envision possible threats but to also discuss what specific actions can be taken. The threatcasting process also allows for us to monitor our success, scrutinizing the indicators and the success of the recommended steps to disrupt, mitigate and recover from these future threats.

In parallel, we will document the Threatcasting Process, capturing the details in a textbook, workbook and video tutorials. The goal is to train the trainers, allowing the process to be taught and run in military academies, universities and in private industries.

The ten Threatcasting sessions and the supporting materials will also serve as a base, when paired with the training tools to enable even greater number of organizations and institutions to conduct their own threatcasting sessions.

The basis of Threatcasting is founded on bringing together diverse multidisciplinary groups to model possible threats with data that is pulled from a diverse set of inputs. Both the process itself and its outputs provide a knowledge base for decisions makers across various sectors. Additionally, the train-the-trainers portion of the project will enable an even wider group of people to participate in threatcasting, expanding the impact of the project.

Another indicator of our success will be how the Lab informs the ongoing debate and discussion for specific action to be taken to disrupt, mitigate and recover from future cyber threats. This can be applied to the military, policy makers, academic institutions as well as industry. Ultimately the Lab seeks to broaden the conversation with the public in general, dispelling the myths and giving people specific visions for the future that are rooted in action.

ACI Actions

The Army Cyber Institute finds itself in a unique position within the military to aid in finding partners to assist with the required research into solutions (many of which will be whole of

government in nature). First, the ACI will socialize the results within the Army Cyber community and the Army's senior leaders in order to provoke internal discussions on strategies, capabilities, and needed force development to be able to operate in these futures. ACI will also work with the military service academies and the Reserve Officer Training Corps (ROTC) detachments to find undergraduate cadets interested to research elements of the findings as projects, capstones, and thesis opportunities within their academic plans. Additionally, ACI will work with the senior service colleges (Army War College, Naval War College, and Air War College) to add this report's findings to their research opportunities for students. This will include working to add some of the described gates to the Key Strategic Issues List that the Chief of Staff of the Army publishes annually. This is in addition to the research that the ACI (along with their rolodex of academic and industry partners) will be able to accomplish. Finally, this is in addition to supporting the Threatcasting Lab at ASU and the 5 year Cyber Threatcasting Project).

Call For Action and Participation

The next Threatcasting session is scheduled for May 1st and 2nd, 2017 at Arizona State University in Tempe, AZ. We are looking for interested parties who would like to participate in the two day workshop and/or have specific ideas and area that require further investigation.

If you are interested, have ideas to share or want more information please contact: ThreatCasting@usma.edu

Conclusion

For many, future cyber threats seem unimaginable and insurmountable. This threatcasting report seeks to envision these threats and empower people and organizations to take action. These possible futures, based on facts and modeled by professionals, can dispel the myths and clear the fog for pragmatic, action-based dialogue.

APPENDIX

Clustering Exercise

Threatcasting Clustering Worksheet	
Team:	Fernando, Julia, Paul, Natalie
PART ONE– Clustering	
Examine the Threatcasting Worksheets and list out the clusters	
	Human in the loop. With the increase in technology and eventual passing of the Singularity Point, we cede more functions to autonomous machines. What skills do we need to retain proficiency in? For what things do we need to stay in the loop over? How do we query machines to explain their decisions if it does not make sense to the human? So, you need to design machines that have a place for humans, that can "dumb down" the machines deicision making so that it can be explained to humans, or "smarten up" humans to understand the machine. Ultimately, must also think about what skills/capabilities that humans need to maintain in case all the machines go dark. This was seen in: Robot Pain Train, Here Comes the Hammer, Detroit X, Logan Has a Bad Day LA
1	
	Rules. There is a need for international norms and rules (inrespective of cultural or social rules/norms). We talked about global issues and global personnas and boundaries in the cyber domain are not similiar to physical domain. These are both rules to deal with bad guys and minimum standards for cybersecurity in tech.These are seen in most scenarios, but specifically in: Health Club Fiasco, Heart of the Sea, Project Mayhem, Infernal Combustion, etc.
2	
	Emergence of diverse future adversaries both in how we think of who they and how they will operate. In general, it will get progressively harder to determine intent from actions as the action surface increases as well as available technology/skills. This was seen in: Robot Pain Train, Health Club Fiasco,
3	
	Data storage and ownership. Who owns what? When do we give up our right to the information and to its protection? This is seen in: Social Panda, Health Club Fiasco, and perhaps was so obvious that many of us did not put into our futures. It will still be an issue 10 years from now .. especially as you add in the idea of PII and what is the next evolution of PII.
4	
	Impact of ever-changing socital/ethical norms; ex. kids today believe that grabbing digital content without paying is okay but still think that taking a candy bar from a store is not ok. Therefore, we are entering an age where actions in different domains have different right/wrong values. This was seen in: Rise of the Social Panda, Health Club Fiasco, Infernal Combustion, the Fall of the Machines, Group 4's un-named scenario from Day 1. WIth the global nature of the cyber domain, you might be talking to someone that is from a different cultural norm/background ... that is also a concern. The problem is the anonymy of online actions and the belief that they wont get in trouble.
5	
	Indirect attack vectors that adversaries are using. For instance, they are not attacking the credit card directly but the refridgerator to get to the same place. This was seen in: Logan has a bad day in LA, Code Red, Project Mayhem
6	
	Micro targeting. The use of micro targeting that is both bad and good.
7	
PART TWO– Backcasting - What can ACI do?	
Examine the clusters	
Explore what needs to happen to disrupt, mitigate and recover from the clustered threats in the future.	
Gates:	

What are the Gates?	
List out what the Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	We develop/influence the behavior of nations. Help instigate conversation on international norms. I.e. UN, NATO. Can we develop what rules should be? "we need to get all the countries to play nice with each other"
2	We develop/influence the behavior of individuals. The Army has a problem with how Soldiers use social media or respond to phishing emails (links). But we combat this through education. ACI can open the aparture of this so that we are not responding to current threats but educating on the future and how the future is changing. We need to work on figuring out how to over-come the ethical right/wrong rules in the cyber domain that new recruits are going to come in with. How do we modify this behavior in individuals? Or how do we change the Army ethic to include this. Start point could be Army intake but should grow/be exportable. "we need to teach every one to be responsible cyber citizens" - education on the consequences of actions in cyber domain with focus on negative; - think about the cultural norms around behavior in cyber domain.
3	Encourage research in decision making of AI, machine learning, and ultimately turn that into output that was human recognizable? Namely, that AI can become intractable to use. "teach machines to play nice with us"
4	Champion a national threat sharing center with established rules ... that apes ISACs but that Joe Smith can report things to. Not really sure if it should be over-arching on all the current ISACs ... but we need something that an individual can report to and therefore, the information gathered can be seen by any individual. "we need to create a community bulletin board for cyber"
5	Exploration of future attack vectors. As the population ages, we take our understandable cues on technology with us and this influences our ability to recognize we are being micro-targeted. Namely, the Publisher's Clearning House example for our parents/grandparents. What are the things that will target our generation? This should be a community experiment. "we need to play the "what if" game (on how we will get attacked as our generation ages)" "determine generational blind-spots"
6	We should use our events as platforms to champion these issues that we are identifying. To promote these goals and to help find others that want to research these ideas to solve these challenges. "our events/outreach should be targeted"
7	
8	
Flags:	
What are the Flags?	*Game changers ... events that can happen that we can't influence that will effect the future; specific things that ACI will keep an eye out that will change or affect the futures we are watching, if they happen - then we can't go back from it and will affect our clusters. If they happen, then we know we are closer to the futures/clusters that we are worried about.*
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	Cyber as its own service.
2	Abolution of European Union privacy laws which could result from either legal battles or (worse case) the collapse of the EU.
3	Global Recession
4	Renounce NATO membership; cancel trade agreements with NAFTA, TPP
5	November 8th, 2016

6	Reversal of net neutrality policy
7	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Identified and partnered with the right stakeholders to affect our gates
2	Develop threat sharing framework for the global community ISAC (bulletin board)
3	Conclude pilot study on "Cyber Citizenship 1.0". Look at previous mis-matches in society (like slavery) .. look at the telegraph (at the double standards of what you can say across the telegraph vice in person). The cultural history could give us the language to talk about it with.
4	
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Develop requirements, specifics for implementation for the global community ISAC (bulletin board)
2	Gain funding from Gates Foundation (un-named NGO with money) for continued cyber hygiene/citizenship development with eventual hand-off to an un-named organization
3	
4	
5	
Notes from discussion:	
	What are social norms that would enable ACI to exist? We dont need full social norms just enough to act and operate as ACI as part of the traditional force. We must study culture to understand how we fit in. We can do the micro of what do we teach cadets ... to what we teach recruits ... but we need to make sure it ties into the larger picture of the nation.
	Group 2: thinks that flags have already happened. We should break activities into tiers (when thinking about tasks that used to be done by humans and now are done by machine) and then each tier has certain requirements (generalistic) about what protection should be included in the system.

	Use of AI and where we would want to have safety and security mechanisms ... the challenge is not robotics but in the next 10 years is dumb AI or functional AI (focused on specific tasks). We are not thinking about developing these intelligence algorithms to optimize a problem but this is what could go wrong. and if you agree with our assessment - then this is the community we need to bring together to think through this. ACI could contribute to this gathering and a study on lessons learned that could be broadened to the general public. Ex was the financial hiccup in 2010 .. that thankfully had a safety mechanism already in place (BDJ wrote a book). We have created resilience in the system that we still crash but recover. Some argue this is erode the system. But ACI - from a supply chain standpoint - that movement of goods or disrupt is a weapon. To give that perspective to folks that are thinking through these issues.
	As automation for supply chain happens and we optimize, how do we also build in validation mechanism that validates the algorithm and that each piece is operating as it should. if you allow if to moderate itself, then it can be fooled. to build a checks and balacnce system so that we are constantly watching. Point of influence of ACI could be ... IEEE, they have rewritten their strategy document to include cyber behavior which will then rewrite policy and then will influence practice. Use IEEE instead of going sector to sector. IEEE has a stick they can carry.
	we talk about transporting military goods from point a to point b, we are using tangible, physical infrastructure. if an attack is there - then you get a cascade effect that can also influence cyber. How do we address/embrace real situations (and their second and third order effects)? it is the intersection of cyber and kinetic. We have to focus on both when we think.
	the failsafe should include a physical component. as we talk a bunch about backdoors and everythign else.. a failsafe can not rely on its own system nor just on a digital failsafe ... this is an extension of the idea of human in the loop.
	as we develop automated systems that rely on electricity, as we add layers of automation - we have to add humans in the loop. Gates - influencing folks on changing policy. Talked a lot about truth and truth management. (Henderson group). need to shore up face to face bonds as virutal communities split us apart from indviiduals that are in our physical location. we are eroding our physical relationships. If we can measure our connectiveness, this could translate into a measure of cyber risk. We tend to fall back on physical resources to help us (local ones) when we are in need. So, how has internet and virtual personas screwed with this.
	ACI could push for (crystal nose.com).... there should be 8 apps that are competing that tell you what information is out there about you (just like there are 8 apps about your credit score). inciting competition to get better products that are needed
	Henderson - ACI can organize and promote fire drills on cyber things. do cyber stand-down day. could be a white card app on your phone that will roleplay it. ACI could start it at installations and then grow it. force people to get an emergency preparedness plan. just like we do for natural diasters.

Threatcasting Clustering Worksheet	
Team:	Sean Griffin, Dan Huynh, Mike McDonald, Brian Schultz
PART ONE– Clustering	
Examine the Threatcasting Worksheets and list out the clusters	
1	Increasing use cases for automation and technology to replace tasks performed by people
2	Increasing social acceptance with giving up personal privacy for convenience or safety
3	The need for adopting standards across policy, security, technology, and safety
4	The need for new technology which facilitates secure communications
5	
PART TWO– Backcasting - What can ACI do?	
Examine the clusters	
Explore what needs to happen to disrupt, mitigate and recover from the clustered threats in the future.	
Gates:	
What are the Gates?	
List out what the Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	develop guidelines and or recommended policy to help shape acceptable tasks which should be automated and what safety measures are applicable; consider interoperability amongst services
2	promote education of future generations to better understand security implications of privacy
3	build relationships with key army leadership and policymakers to become recognized as a credible source for cyber expertise
4	
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	robots / drones used to kill in both war and in domestic scenarios has already happened
2	

3	
4	
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	On automation of task and use or robotics:
1	engage companies to look at where safety mechanisms should be emplaced
2	use lessons learned from High Frequency Trading / stock market crashes to apply to other sectors
3	conduct study to help identify and apply to supply chain
4	impact IEEE hardware specs / policy
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	
2	
3	
4	
5	

Threatcasting Clustering Worksheet	
Team:	Steve, Glenn, Rob
PART ONE– Clustering	
Examine the Threatcasting Worksheets and list out the clusters	
1	Keeping the human in the loop
2	Hardening of the internet ... mission critical utility
3	Cyber resilience of systems and self-diagnosis/validation
4	Known and Predictable Human behaviors and interests still "drive the train" despite being sometimes obscured by technology.
5	Reality management (reality assessment) is really important as many physical/life-death decisions hinge on determining what is real and legitimate. Automation and virtualization can inflate, obscure, alter reality
6	Data Ownership. Ubiquitous cloud-based storage of all data by third-parties has vast implications on privacy, anonymity, and vulnerabilities. Individuals can't opt out
7	Hacking (intrusions, exploits, etc) will always happen and will scale linearly in the future. Cannot/will not be eradicated. Levels of attack and ability to defend will stay at their current balance (but is this a good assumption)
PART TWO– Backcasting - What can ACI do?	
Examine the clusters	
Explore what needs to happen to disrupt, mitigate and recover from the clustered threats in the future.	
Gates:	
What are the Gates?	
List out what the Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	We need to influence the people in power for policy purposes, with the main goal of working with people who already agree with our general goals, but whom are powerful and can leverage major industries (e.g., trade groups) who can listen-to and integrate our guidance.
2	Stump for international standards for automation and human control. Develop metrics (via organizational psychology & systems engineering) to test and understand the correct level of human control and redundancy.
3	Focus on standard for end-to-end encryption to protect critical infrastructure, especially in the future IoT with increased automation.
4	NIST/SISO Truth System. Develop a vetted, democratically backed, secure, transparent "black box" fact checker that uses AI to score knowledge/data/information as to its probability of being true. Controlled and owned by the people. Manage design and tuning so that it stays as objective as possible. This is information assurance, but needs to be global, real time in some cases
5	Argue for policy where people 'own' their own data and online presence. 'rent' online data with safeguards for deletion. UK's right to be forgotten.

6	Shore up and strengthen physical face to face bonds and interactions among people living in physical communities and work areas. This creates a backup social construct that will endure after a Cyber 9/11 and be resistant to cyber hacking
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant effect on the futures you have modeled.	
1	Automatic vehicle hacked / Amazon supply chain hacked (Cyber 9/11). Until a major cyber-enabled corporation experiences a major blow to their bottom-line, things won't change much
2	Major advance in automation that enables automation to self-organize, self-maintain at a level that makes human oversight irrelevant and very expensive. If this happens, then there will be insurmountable pressure (economic, technology) to get the human out of the loop
3	Election hack or information hack around the election that causes people to question legitimacy or cause loss of international prestige
4	Pokemon Go gets hacked, people's lifestyles documented and predicted with a higher degree of resolution.
5	We reach a tipping point where geographic communities and local relationships are non-existent because the majority of influential, accepted, and "trusted" social communities are 100% virtual (and thus highly susceptible to hacking)
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and prepare for recovery from the threat?	
1	Organize and promote cyber drills and pedestrian pen testing at the national level. Promote cyber-readiness and resilience to reduce fear and induce trust in the system. This is akin to national drills during the cold war, but more effective and based on reducing threats through changed behaviors
2	Develop the set of international rules (ala NIST) for big data privacy and big data use.
3	Policies in place for establishing the appropriate level of human-in-the-loop interaction and need for local redundancies in political, economic, transportation, healthcare, military processes. Create a model that can (a) measure the ratio of automation/human redundancy in a given system (in a general sense that can be ported across many domains) and (b) establish minimum acceptable ratios for various categories of systems. For example, certain critical systems might require a minimum ratio of human redundancy
4	Push for encryption standard in IoT devices.
5	Develop metric for measuring the ratio of virtual communities to local/physical community in a geographical area. For example, if the people living in Hamilton, OH have 90% of their relations and social interaction with people outside Hamilton is this community resilient to hacking/BigData manipulation? How can governments, policy makers and community leaders alter this? Having a metric for understanding the problem is an important first step.
What needs to happen in 8 year to disrupt, mitigate and prepare for recovery from the threat?	
1	Extend cyber drills to megacities. Go beyond army readiness to national readiness.
2	

3	
4	
5	

Threatcasting Clustering Worksheet			
Team: John, Carlos, Ali			
PART ONE– Clustering			
Examine the Threatcasting Worksheets and list out the clusters			
1	Human in the Loop		
2	Hardening of the Internet		
3	Automation Backdoor Access - building in failsafes for the automated systems we have created		
4	CRISPR for code - modifying code to shift intent or application of technology rather than changing the core of the technology itself		
5	Behavior modification through misinformation. Systems engingeering: intentional delay based on lack of feedback. Exploiting the gap in information - the gap between real and synthetic reality. We need to find a mechanism to find an analyze decisional data faster (validate the reality). how can we make transparent the behavior change be monitored by searches		
6	Trust in the system. At what point on the spectrum from real to synthetic is the tipping point where we lose trust? How do we correct the margin of error? If I defer to the machine am I protected/rewarded/wrong?		
7	Transparency to allow grassroots decisions. Not transparency over a global system, but across the local systems in use. Generating a global system creates a single point of failure. There is an advantage to creating a decentralized system (opposite of TPP).		
8	Behavior, political, and tactical changes start virally and disseminate outward, rather than taking a top down strategic plan approach. note: mgmt not ready to tackle strategic changes (as mentioned by Fernando)		
9	Open source big data pulls introduce many points for misinformation. Aggregating many "false positives" through data feeds can severely disrupt larger systems which are implementing this infomration without secondary checks.		
10	Unclear cyber boundaries. Ethics, behaviors, expectations, and legislation need greater definition in order to govern national and international relationships.		
11	Integration of tech advancements in "dumb" society creates social tension and potential harm. Artificially creating a caste society (haves / have nots)		
12			
PART TWO– Backcasting - What can ACI do?			
Examine the clusters			
Explore what needs to happen to disrupt, mitigate and recover from the clustered threats in the future.			
Gates:			
What are the Gates?			
List out what the Blue Team has control over to disrupt, mitigate and recover from the threat.			
1	ACI has ability to shape IEEE strategic plan for cyber and hardware security/transparency standards - currently governed through piracy, finacnce, and access (who owns) the data		
2	Construct backdoor access to all automated systems (accessible by a human)		
3	Cross-agency data collaboration. Comparisons for similarity, repetition, and duplication.		
5			

5			
Flags:			
What are the Flags?			
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.			
1	Expansion of identity definition (e.g. gender to spectrum, splintering online identities, or multi-person shared identity)		
2	Conviction of a group identity, those in the group identity share responsibility		
3	Proliferation of disposable tracking (wearables)		
4	Mass exodus from some component (social tool, part of cyber environment of any kind)		
5	Massive data breach tied to an experience or specific location which is immediately felt, pervasively catastrophic and changes behavior of those effected ~150k members (i.e. Bangladesh; e.g. bank accounts wiped for everyone in NYC)		
6	Hacking of a benign product, changing it for malignant purposes		
7	Society recognizes responsibility as shifting from the human (driver) to the machine (car) or cyber agent		
8			
Milestones:			
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?			
1	Develop a set of norms we are comfortable with third parties collecting from us (and our families) - for app developers		
2	Identity tokenization (attribution of known personas)		
3	Create data access notification system in order to see an overview of personal data and who has accessed it (e.g. credit score for data usage)		
4	IEEE published standards for hardware and cyber protocol		
5	Develop automated system, fail safe aspect includes human in the loop (moderate monitoring by human)		
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?			
1	IEEE implemented standards for hardware and cyber protocol		
2	Digital governmental approved identity system (virtual and physical identity integration)		
3	Create unified shared data stream for all government agencies		
4			
5			

DAY ONE:
Threatcasting and Backcasting Workbooks

Threatcasting Worksheet	
Team:	Julia Rose West, Andy Hall, Natalie Vanatta, Josh Bundt
Experience Title:	Health Club Fiasco
Estimated Date:	2026
Data Points	
Slot #1	Social status is really important and influences more than we assume
Slot #2	True Sentinent Beings?
Slot #3	Automated decision making (systems making decisions for us)
Slot #4	Professional licensing for developers
Slot #5	Information Flow (disrupting infomration flow will delay supply chain, which will break trust)
Slot #6	Asymmetric adversary attacking soft targets (targeting familes and love ones to impact will to fight)
Slot #7 (This is 2020)	Device security rules (poor device security continues as tech solutions rush to market)
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Asim owns a gym in Bahrain. Married with a wife and two kids (two boys, 10 and 12). This is a family business and he is teaching his children about the fitness business. His father is a local cleric. He wants to grow his business and open two more gyms this year. His father's social status influences him. His wife runs the gym's website and social media and is a software engineer. It is a high-speed gym where apps are tracking medical conditions and reps ... they wear smart shirts to workout in. He has customer DNA and health data - he maps it to create the perfect gym experience for them. This information is also stored online so that customers can see it / access it.
Where do they live?	Lives in Bahrain
What is the threat?	someone (external) steals all the customer data for targeted retribution / blackmail for persons of prominenance
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	

What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
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 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 new capabilities enable the person and their broader community to recover from the threat?	
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?
	Asim gets a video (or hologram) from the sub-culture hacker group that targeted him that are against mixed tribe individuals in order to create a more pure society. They want him to know they have all his records in order to cause fear and chaos in his customers. They are threatening to make a big scene so that his father's standing as a cleric is affected. Asim is pissed with his wife since he blames her as the social media and website guru. He blames her selection of the various apps that had vulnerabilities that allowed the hacker group in. This causes distress in the family (but he does NOT beat his wife). They are considering moving but his parents are too old to go with them. They lose trust in their clients and community because of the various secrets that are exposed. Other concern is that US servicemembers are some of the customers affected. They are used to using health facilities in the US and expect a level of cybersecurity.
Question Two	What new capabilities enable the person and their broader community to recover from the threat?
	CRISPR - gene modification for those that can afford it (fixes DNA stolen); nothing fixes that people know you are mixed tribal
PART THREE: Enabling Questions - **Red Team** (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	***New Practices: What new approaches will be used to bring about your threat and how will the Red Team enlist the help of the broader community?***
	Any hack can be purchased for the right amount of money. Hacks are a commodity item. They are an ideological group so bring a scientist over to their side to help with the analysis of the DNA results. They could also hack the thrid party of ancestry.com
Question 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?***
	As a ideological hacking group, they get top cover from supporters in the national and local government who look the other way when they terrorize citizens. they are bringing back the true faith and pure tribe.
PART FOUR– Backcasting - **Blue Team** (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	ability to put things off limits (dont let service members use the gym) - but this has a negative effect on relations with the country
2	
3	encourage use of best practices in cybersecurity to local businesses; host training sessions as outreach

4	change the methodology - you bring your data and process data locally but not leave it with the facility .... they provide the algorithms to crunch your data but you retain the data
5	Similar to transgender folks associating with a certain gender - there could be tribe associations or region associations separate of what DNA reveals.
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	DNA is out in the cloud; can never recover or prove it is you (in future felony cases)
2	can't influence Bahrain government regulations to encourage tighter cybersecurity
3	Service members choose to use foreign local services
4	
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	change culture for individuals not to so willingly give up their DNA ... (where extra information is not provided when not needed)
2	develop international standards for software development to adhere to cybersecurity smartness
3	change the model for data ownership; privacy is maintained through DNA? companies no longer are allowed to own customers data, they must pay/rent it.
4	
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Research shows what uniquely identifies an individual (DNA may not uniquely identify someone when DNA can be 'edited').
2	
3	
4	
5	

Threatcasting Worksheet	
Team:	Fernando Maymi, Rob Thomson, Alida Draudt, Steve Henderson, Rob
Experience Title:	RISE OF THE SOCIAL PANDA
Estimated Date:	2026
Data Points	
Slot #1	There is no one general system to detect threats and opportunities; our minds are not developed to do deep thinking so we need time to think through things
Slot #2	Smart & Trusted Objects (e.g. Smart Shirt)
Slot #3	Misinformation as a weapons system
Slot #4	Engineering practices
Slot #5	Supply Chain Ecosystem
Slot #6	our adversaries are digital natives
Slot #7 (This is 2020)	Hackers go mainstream
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Li, a mainstream hacker (aka Darc Diabl0)
Where do they live?	Singapore
What is the threat?	THREAT: SocailPanda, a national citizenship score, originally based on a "credit score"; A single score, controlled by the State, linked to gamified social media, online shopping, entertainment to build loyalty, convergence, control; No ability to lead divergent hacking life AND have a good score
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	

	Avoid compromising state sponsored citizenship score but keep freedom of action to hack
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 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 new capabilities enable the person and their broader community to recover from the threat?	
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?
	Social Panda has been online for one year...Tension between two lives causes gradual loss of credit; Then, Li finds out (after the fact) that they were left out of social opportunities; Wasn't invited to his friends party; Checks score, hypothesizes new data source has been added to SocialPanda. Hasn't slipped, realizes duality becuase system is mining data and rooting/squeezing him out. Must figure our what new data set is.
Question Two	What new capabilities enable the person and their broader community to recover from the threat?
	Reverse engineer software protocols to overcome system. Man in middle to get ubiquitous devices to provide false information to cover social score. Band together with other hackers to use smart tools and apps (fueled by AI) to do this for him. Code a second persona that hacks SocialPanda to duplicate a false "proper life." Hack the next data source process to be included in the SocialPanda to control system. Last resort: Grab the cyber hammer and start swinging for the bleachers.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	

Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?		
Question One	New Practices: What new approaches will be used to bring about your threat and how will the Red Team enlist the help of the broader community?	
	SocialPanda is a government-backed, self-sustaining system based on social incentives and behavior. Add more and more data.	
Question Two	Ecosystem Support: What support is needed? What industry/government/military/local partners must the Red Team team up with?	
	An initial algorithm to define a covgergent score (what is a good citizen)? Partner with the data sources (AliBaba, google.sg, community sensors, neigborhood watch)	
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)		
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 Blue Team has control over to disrupt, mitigate and recover from the threat.		
1	Control over other hackers	
2	Can identify companies pulled into SocialPanda	
3	Erode trust in the scoring process (point out social inequality)	
4	Create counter culture	
5		
Flags:		
What are the Flags?		
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.		
1		
2	75% Penetration of IoT via Wifi or other ubiquitous netowrk	
3	Government gains ubiquitous access to IoT Data	
4		
5	Deployment of SocialPanda	

Milestones:		
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?		
1	Corrupt data sets to build in BigData backdoors	
2	Citizens own their own data (litigation)	
3	Promotion of open-source social media networks	
4	Counter-measures to mass social engineering	
5	Prepositioning the tools and education	
6	Encourage and online many personalities per physical person	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?		
1	Development of sizable hacking force	
2	Create small hackathons	
3		
4		
5		

Threatcasting Worksheet	
Team:	Erik Dean, Glenn Robertson, Clint Watts
Experience Title:	The Fall of the Machines
Estimated Date:	2050
Data Points	
Slot #1	Many of our cues we inately use are from our evolutionary past; evolutionary cues and environmental cues
Slot #2	Manipulation of Social Media (China Gamified CitizenNet)
Slot #3	Automated decision making
Slot #4	Engineering practices
Slot #5	Emerging tech like robots, 3D printing, IOT
Slot #6	Asymmetric adversary attacking soft targets
Slot #7 (This is 2020)	Cybersecurity is at the threshold of profound psychosocial impact.
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Hans Gruber the average German citizen - works in a completely automated factory with touch labor ONLY for maintenance and upgrades
	Wife Gretel, Brother Simon
Where do they live?	Germany
What is the threat?	Changing socio-ecconomic and demographics of his home town due to influx of refugees from Middle Eastern country
	Attack on automated systems and misinformation about ethic group of refugees causing the attack
Briefly describe how your person experiences the threat.	
Crumbling of EU and NATO in addition to rising influx of non-Germans causes coupled with rise in automation and robots has caused a significant loss of jobs which are being taken by cheaper labor or robots.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
The person's entire family and community are involved. The Red Team hopes to destabilize the region by disrupting automated manufacturing. The cheap labor has caused an untrained workforce that does not know how to run manufacturing when machines and automation are not operational. The Red Team is hoping to foment turmoil inside Germany and to weaken the economic strength of Germany as well as to drive manufacturing to a Red Team friendly country. The Red Team is not frightened of anything.	
What is the experience we want the person to have with the threat?	

We want the Red Team to fail and the economy to remain stable as well as the relationships with all soci-economic groups to remain smooth and get stronger.	
We want second generation of immigrants to integrate into surrounding culture	
What is the experience we want them to avoid?	
Economic collapse in Germany + fear of other social, economic, ethic groups	
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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	**"The Event" - How will your person first hear about or experience the threat?**
	He has lost his job due to automation or is under competition with cheaper labor, taxes have gone up to pay for additional social services. They will hear information from other nations amplifying the threat and inciting fear and instability.
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)**
	Hans will see the threat firsthand as well as see/hear information through TV and radio. Hans will talk with others, in person, in his community.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
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 Red Team must reach Hans via a trusted information source with false or biased information. The Red Team must disable or degrade automated capabilities forcing panic.

Question Two	***Business Models: What new business models and practices will be in place to enable the threat?***
	With the rise of automation, most companies have moved away from manual labor and are using completely automated systems for production.
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
	Counter mis-information through rapid media dissemination
2	Development of social and government crisis response plans
3	Provide social integration and stabilization support
4	Ensure redundance in automation capabilities
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	Mass protests of different income classes against socio-economic changes + polarization of associated groups
2	Outages of large distributed computer systems
3	Change from any touch labor during manufacturing to complete, end to end, automated process
4	
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Communicate resiliency and response plans to the public and openly test them frequently
2	Ensure manually-operated backup systems are available for all automated systems
3	Create a redundant "copy" of every critical system to be used as needed
4	
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Change the media's messaging (including TV shows and movies) portraying the worst possible outcome to all situations (ex The Walking Dead)
2	Create systems that can completely verify their integrity and the integrity of the data being used
3	
4	

5	

Threatcasting Worksheet	
Team:	Paul Maxwell, Rock Stevens, Adam Duby
Experience Title:	
Estimated Date:	2026
Data Points	
Slot #1	Social status is really important and influences more than we assume
Slot #2	Living off the Grid
Slot #3	Misinformation as a weapons system
Slot #4	Engineering practices
Slot #5	Supply Chain Ecosystem
Slot #6	our adversaries are digital natives
Slot #7 (This is 2020)	Cybersecurity is at the threshold of profound psychosocial impact.
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Sergei Romanov Criminal hacker, financially motivated, famous hacker pseudonym
Where do they live?	London
What is the threat?	Distruption to his way of life and income
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	

	Primary threat to Sergei is attribution of his illegal activities and imprisonment. LE is afraid of tipping Sergei off and pushing him further underground or changing modes of communication (strong encryption etc) Sergei lacks trust; experiences spike in paranoia when his network has data usage spikes when he's not logged in, notices white van parked outside. Social exile; recluse; isolation
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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	**"The Event" - How will your person first hear about or experience the threat?**
	Online associate is v&'d (vanned), Sergei receives anon tip that he's being targeted next
Question Two	**What is different and/or the same as previous events or instantiations of the threat?**
	Sergei is a digital native and expert -- harder to target; systems are harder to exploit and attribution obfuscation is more impossible; Sergei is using different initial entry points into network (never attacks from the same phy location); he has a strong distrust of hardware and IoT devices --> pushes him further away from the connected world)
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**
	Attribution tools like BEEF that disclose victim's IP/geolocation; policy levers that can target institutes that support criminals/spammers (e.g. CMU spam analysis white paper); controlling TOR exit nodes to disclose traffic patterns
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/local partners must the Red Team team up with?**
	hardware manufacturers with backdoors; ISPs willing to disclose traffic logs; stigmatize criminal underground (society support against the practices); cell phone tracking; require on-the-grid dependencies (with unique logon requirements)
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Misinformation as a weapon -- moving targets to remain hidden; create fear that gov is going to deny liberties via tracking tools
2	Criminals want to foster false sense of security to make their job easier -- "hacking is hard, we're more secure now, don't worry about it"
3	Disrupt international cooperation -- masquerade as nation-state attacking other allied nation-state (a la Merkel)
4	Pro-hacker campaign -- showing benefits to the world that hackers bring (wikileaks, counter-ISIS, Equation Group auction etc)
5	
Flags:	
What are the Flags?	

List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	International norms, treaties over hacking
2	Built-in gov-controlled backdoors
3	Removal of anonymity from web (signed actions, bread crumbs)
4	Growing sec awareness
5	More mature software and hardware design practices
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Build better anonymity tools
2	Build attacks at scale to increase income and harder to detect; cast wider net
3	New revenue models --> big data blackmail
4	Support EFF / ACLU
5	New ways of laundering money
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Spoof online attribution --> fake IDs
2	
3	
4	
5	

Threatcasting Worksheet	
Team:	Mike McDonald, Chris Arney, Chris Claremont
Experience Title:	Code Red
Estimated Date:	2026
Data Points	
Slot #1	Context affects perception; how vulnerable you feel is based on other threats in your environment; some situations you would be hyper-vigilent but you can't always be (change in your posture based on whether at work than home)
Slot #2	True Sentinent Beings? True Sentinent Beings will not exist in 10 years or (probably) even 20; Too brittle to achieve true sentinent standard; But we will be able to do limited cognitive modeling
Slot #3	Commanding Data & App Creation. Autonomous devices will generate data and do things on their own. Apps are being generated autonomously by large platforms. How do we control these? Corporate entities will command platform, we will suscbribe to effects.
Slot #4	International norms/establish policies that discourage malicious actors. Is CNE acceptable? Does cyber espionage change the spy game?
Slot #5	Supply Chain Ecosystem. Suppliers have suppliers have suppliers. A weak spot in any one of these systems has massive cascading effects on the whole ecosystem. There are national security implications to this, as well. Recent examples include the F-35 breach through subcontractors and Qualcomm chip hardware vulnerabilities, exposing millions of Androids.
Slot #6	Our adversaries have unprecedented knowledge of our TTPs. Adversaries can easily identify our equipment and personnnel security vulnerabilities, patterns, and MO and exploit them,information disclosure, messaging.
Slot #7 (This is 2020)	Cybersecurity is at the threshold of profound psychosocial impact. Cyber Security's impact on the public psychology erodes trust in the financial and other systems that form the building blocks of modern society.
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Woman, mid-40's, non-college grad, digital native, veteran, hardware repair, public sector employee
Where do they live?	Chicago

What is the threat?	Foreign commercial entity in competition with the domestic medical technology provider (insulin pump); hacked system to destroy consumer confidence in domestic product, neutralizing competition
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
	She's a nurse who distributes the insulin pumps and doses; feels responsible for people dying due to "glitch" with the domestic product. Families of deceased people, colleagues, spouse, device manufacturer, FDA, police/FBI. Implication in an act of war - deliberately killing civilians for commercial success. She figures out that the glitch is a hack, not a glitch. We don't want her not to figure it out.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	"The Event" - How will your person first hear about or experience the threat?
	She's a critical care nurse and a number of patients suddenly die due to insulin pump failures.
Question Two	What new capabilities enable the person and their broader community to recover from the threat?
	Because she doesn't have degrees, she's underestimated. She sees things from a more immediate and personal perspective that the FBI doesn't have insight to. She keeps getting blocked from investigation from the device company, the FDA, the FBI, etc.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
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 competition's government, international law, domestic authorities and agencies, domestic competition
Question Two	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**
	Insulin pumps - smart insulin pumps that receive/transmit data to manage insulin automatically.
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Identity the problem/source
2	Reveal the true source of the problem to the US vendor and the authorities
3	US vendor patches the system, but doesn't want to reveal the source code or admit publically it was hacked by a foreign power
4	FDA must conduct a top-to-bottom anaysis of insulin pump source code to patch vulnerabilities
5	The Chinese gov't punish the top brass of the company/wipe it out with US pressure to maintain relations/trust, but keep the code for future use.
Flags:	
What are the Flags?	

List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.		
	1	Foreign supply chain management
	2	International jurisdiction/authorities
	3	No subpoena power (for the hero)
	4	No support staff
	5	No access to official assistance
Milestones:		
What needs to happen in 4 year to disrupt, mitigate and prepare for recovery from the threat?		
	1	CIA/NSA/FBI/DHS/FDA must continue to be vigilant in looking at code anomolies/malware
	2	Recruiting as many hackers into government agencies to be white hats as possible
	3	Continue to monitor the same enemy and enemy allies
	4	Conduct hackathons and bug bounties to continue to search for vulnerabilities
	5	Possible economic sanctions?
What needs to happen in 8 year to disrupt, mitigate and prepare for recovery from the threat?		
	1	CIA/NSA/FBI/DHS/FDA must continue to be vigilant in looking at code to ensure vulnerabilities are patched
	2	Massive civilian education in STEM
	3	AI-assisted malware detection, mitigation, and recovery
	4	Increase use of domestic supply chain/decreased reliance on foreign products/supply chain
	5	

Threatcasting Worksheet	
Team:	Bill Cheswick, Dan Huynh, Carlos Vega
Experience Title:	Project Mayhem
Estimated Date:	2026
Data Points	
Slot #1	Beware of your short term bias(s); our brains are not designed to think long-term; we like to think the past is also the future
Slot #2	True Sentient Beings?
Slot #3	Misinformation as a weapons system
Slot #4	International norms for self-securing
Slot #5	Supply Chain Ecosystem
Slot #6	Our adversaries have adaptive distributed networks
Slot #7 (This is 2020)	Cybersecurity is at the threshold of profound psychosocial impact.
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Bobbie Paulson; wife of SFC Robert Paulson; typical American family; 3 children
Where do they live?	Springfield, Indiana
What is the threat?	Attack on social structure; reduce of effectiveness and morale of forward deployed troops with no risk to attacker
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
	Use of social media to portray a false story of infidelity of spouse; hacking into spouse and service member accounts

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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	**"The Event" - How will your person first hear about or experience the threat?**
	-testy phonecall from the frontlines questioning infidelity and trust of spouse
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?**
	-confusion, hurt, unjustified
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	
	New Practices: What new approaches will be used to bring about your threat and how will the Red Team enlist the help of the broader community?

	-using social media sites to propogate a story line
Question Two	
	Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?
	-understanding social culture, developing effective social engineering techniques
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	train servicemembers and families about these attacks to better prepare them
2	develop a social media aggregator to help create awareness of your digital persona
3	provide robust and persistent communication mechanisms
4	
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	increased number of suicides for deployed soldiers
2	realization that a third party adversary is interfering with spousal relations
3	congressional inquiry initiated into these incidents
4	discovery of ISP man in the middle attacks on service members and families
5	realization that adversaries are engaging soft targets (spouses of deployed service members)
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and prepare for recovery from the threat?	
1	develop social persona aggregation technology
2	push for the implementation and distribution of usable encryption for home use
3	develop policy that prohibits the use of unsecure communication for home use

4	deploy usable security for social media sites and home use
5	public awareness campaign
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	develop uniform standards and policies for secure communications
2	develop uniform standards and policies for auditing and monitoring
3	establish international norms for targeting civilians
4	
5	

Threat Casting Worksheet	
Team:	Brian Schultz, Sean Griffin, Rhett Hernandez, Gus Rodriguez
Experience Title:	Turning Off the Lights
Estimated Date:	2026
Data Points	
Slot #1	Context affects perception
Slot #2	Smart & Trusted Objects (e.g. Smart Shirt)
Slot #3	Micro-Targeting
Slot #4	International norms / establish policies that discourage malicious actors
Slot #5	Supply Chain Ecosystem
Slot #6	Asymmetric adversary attacking soft targets
Slot #7 (This is 2020)	Hackers go mainstream
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Hank Simpson
Where do they live?	Chicago, IL
What is the threat?	Micro-targeting, Social Engineering, Compromise his system, gain access to plant ICS
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	

	Red Team conducts recon on Hank through Social Media and targets him with phishing email in order to compromise his personal computer at home, unbeknownst to Hank or his family. Hank uses this system to VPN into the Power Plant in order to monitor ICS systems on the weekend. The Red Team wants to gain administrative access to plant control systems. Red Team is hoping to gain a foothold at the plant to shut down the power. The Red Team is frightened of discover and attribution.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	***paste question here***
	"The Event" - How will your person first hear about or experience the threat?
Question Two	***paste question here***
	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)
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	

Question One	***paste question 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?
Question Two	***paste question here***
	Ecosystem Support: What support is needed? What industry/government/military/local partners must the Red Team team up with?
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Implement 2-factor authentication
2	Network Segmentation
3	Secure Remote Access
4	User Education: Minimize Digital Footprint
5	Monitor and Respond to Infiltrations on the Network
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant effect on the futures you have modeled.	
1	The human element
2	The increasing interconnected nature of our devices
3	Decrease of personal privacy; both voluntary and involuntary
4	
5	
Milestones:	

What needs to happen in 4 year to disrupt, mitigate and prepare for recovery from the threat?	
1	Techinical Controls: Emplace some form of enhanced authentication (Biometrics, etc.)
2	Outreach: Improved Cyber Intelligence sharing with local authorities to encourage shared responsiblity
3	
4	
5	
What needs to happen in 8 year to disrupt, mitigate and prepare for recovery from the threat?	
1	Legistlate: A separate purpose built network to connect 3200 power plants in the nation (i.e. Internet 2)
2	Education: General Cybersecurity classes starting at elementary level to prepare future workforce for Cyber threats
3	
4	
5	

DAY TWO:
Threatcasting and Backcasting Workbooks

Team:	Team Awesomeness: Julia, Josh, Andrew, Natalie
Experience Title:	The Robot Pain Train
Estimated Date:	2026
Data Points	
Slot #1	There is no one general system to detect threats and opportunities; our minds are not developed to do deep thinking so we need time to think through things
Slot #2	Commanding Data & App Creation (Autonomous devices will generate data and do things on their own. Apps are being generated autonomously by large platforms.) (Apps continously evolving without human interaction)
Slot #3	Micro-Targeting (ability to hide our folks will be more difficult but ability to provide better targeting data to limit impact to bystanders)
Slot #4	International norms / establish policies that discourage malicious actors
Slot #5	Information Flow (disrupt the information flow to break trust)
Slot #6	Asymmetric adversary attacking soft targets
Slot #7 (It's the year 2020)	Device security rules (Poor device security continues as firms continue to rush technology solutions to market.)
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Nurse Jackie lives in San Francisco and has devoted most of her life to helping people. She started life as a nurse and had a revolutionary idea on how to make patient care better but limited tech skills. She created a company and is the CEO. She has 100+ people working for her now. They developed tech and software to "read human minds" to get a better handle on pain and phsyiology affecting the patients in order to provide better care. They can then use a combination of drugs and modification of brain patterns/waves to eliminate pain. Now that they have figured out a way to effectively remove pain, other foreign actors want this tech to enslave their dissidents. Their latest product is an in-home robot that can do this. This idea took off so well that many hospitals are also using this technology and abandoned some of their old ways to do pain management.
Where do they live?	San Francisco, CA

What is the threat?	Bad actor can insert malious code into new components of the robots. The concern is a targeted attack as the first generation owners of robots (folks with lots of money) who are now replacing and upgrading to the latest.
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
	The threat is against the robots that are doing the in-home care. The signularity point is approaching and this group is using robots to attack people to show the world that robots are bad/harmful. This is a domestic group.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
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?***
	Nurse Jackie sees newspaper reports of the robots malfunctioning and medically disabling the patients by turning up the pain (vice turning it down). She also starts to receive complaints by loved ones of individuals using robots. There are also news stories from this group (while not claiming responsibility) - they are spinning about how this is bad and proves their point. Lots of OpEds on this. There seems to be no explanation on why this is occuring. Jackie is frantically callign her technical staff together to begin analysis on what is going on. FDA is also involved. The scene is frantic as human's lives are being affected (there are multiple news stories with old folks and children in pain being shown). There is such a prevasiveness of this technology that they are not initially sure how to re-call or roll back. What they don't see or understand initially - is where this all happened, what caused it ... what is malicious (software or hardware). No one thought that someone was taking over the robots - it was first assumed that the robots were the malicious actor ... somewhat based on what the spin in the media and this group was doing.
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)***

	So, FDA strongly recommends shutting off the robots but the issue is that the hospitals are not able to cover down on the medical requirements because they have also switched to robots to handle pain management. THere are not adequate supplies of drugs or trained personnel to handle the need for pain management in the city. There is a bit of a panic and governor calls for state of emergency as these robots are not just used in San Fran but also throughout the major metro areas in the state. Nurse Jackie reaches out to FBI Cyber Division to assist with the analysis on what is causing it. They ultimately determine it was an issue embedded in the second generation chipset that is manufactured in a foreign country. At this point, other government agencies reach out to assist with determining feasible solutions to fix. The hardware was subverted ... the actual code and communication with the devices was secure.
PART THREE: Enabling Questions - **Red Team** (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	***Ecosystem Support: What support is needed? What industry/government/military/local partners must the Red Team team up with?***
	The bad guys group are primary domestic actors. They have to have one or more of the component makers co-opted to their cause. (very similiar in nature to ISIS and their call to create a caliphate). They would need a strong PR person and narrative creators in order to develop a recruiting campaign. They also need folks in national media outlets to ensure that they opinoins are printed and the actual news story makes the edition. They also have supporters in the VA to ensure that many of these robots get into america's veterans homes to help their cause. They have also co-opted some congressional staffers to influence their principles to support legislation to take robots out of all homes, schools and critical, key infrastructure. Schools because many school nurses are replaced also. This legistration was written prior to the start of their execution of attack.
Question Two	***New Practices: What new approaches will be used to bring about your threat and how will the Red Team enlist the help of the broader community?***

	Bad guys are using on board sensing capabilities of the robots and creating an online presence that is being populated by the robots as if the robots are tweeting "haha ... just killed this person". They are also looking for instances where people had a bad reaction to autonomous vehicles/things and targeting them to get the corrupt robots. These individuals would be radicalized to their cause. The bad guys also create a pro-human movement that seems good to convince others to help and support. This group also used social media and intel gathering techniques to figure out who to turn within the manufacturing company vice planting their own. They also initially used cyber attacks to change data within contracting processes to ensure that their preferred manufacturers came in with low bid to initially make the chips.
PART FOUR– Backcasting - **Blue Team** (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Engage with the group to limit their radicalization. FBI should have lead/responsibility on this. There was a long tail leading up to the attack that they could have been noticed and stopped.
2	Find ways to test chipsets and upgrade parts on robots. Better Q&A that is regulated. The issue is figuring out how to do adequate tests as the systems are so complex. This is the verification as they come off the line.
3	Develop ideas for dual-monitoring for system overrides; for being able to query the robot on what they are doing and why they made the decisions that they did.
4	Create a better counter narrative - "pro-teaming" concept. Re-design the robot to make them more friendly to humans (change perception) .. perhaps it also consoles you when you are hurt. (21st Centruy Robots)
5	Determine a way to create a "safe list" of manufacturers that are routinely monitored for not implementing back doors or malicious code into products for others. This could be a similar setup to how we do nuclear inspections of foreign powers.
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	Can't contol people's feelings on natural technology evolution/progression. this undercurrent will always exist that the bad guy group tapped into.
2	Natural economy forces us to become more dependant on AI and robots in the future. Can't go back.
3	Can't stop all hacks or malicious actors. Even if we have a bunch of regulations, reviews, and other mechanisms in place. Nothing will catch everything.

4	Can't affect the length of recovery from the threat. Because we have out-sourced alot of our manufacturing capabilities and what is still in the world is tied to current demand. This threat requires us to replace all robots which would be a significant increase in demand ... so it will take a bit. Especially as we want to ensure that it does not happen immediately again to the same robots.
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Meaningful public debate concerning the development of robot / AI technology -- limits, public policy, safe guards
2	Development of some domestic manufacturing to reduce dependence on international chip manufacturing.
3	Minimum number of trained and educated emergency services personnel to be prepared to react to natural and/or manmande diasters and take over the reposibilites of the robots. Assume that someday robots will go dark - what do we need to be able to do without them (after we have out-sourced our capabilities).
4	Determine a way to help identify potential citizens that could be radicalized and help provide options that meet their needs without the radical group. This could be applied to all folks - not just this group.
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Develop a framework for inspection of chip manufacturers. Develop a program that benefits companies that use these manufacturers and manfacturers that join the program
2	Encourage research into how do we query robots/autonomous systems to explain their decisions when they dont make sense to the humans. Especially as problems and decisionmaking is just getting more and more complex.
3	
4	
5	

Threatcasting Worksheet	
Team:	Fernando, Ali, Rob, Steve
Experience Title:	Here Comes the Hammer
Estimated Date:	2026
Focus on a person in commerece working in a dense urban areas and how does cyber threat make it into the physical world. OUTBRIEF-->More detail. (1) Experience (2) Most useful (3) What can the ACI start doing today to disrupt, mitgate, recover	
Data Points	
Slot #1	There is no one general system to detect threats and opportunities; our minds are not developed to do deep thinking so we need time to think through things
Slot #2	Commanding Data & App Creation
Slot #3	Micro-Targeting
Slot #4	International norms / establish policies that discourage malicious actors
Slot #5	Information Flow
Slot #6	Asymmetric adversary attacking soft targets
Slot #7 (It's the year 2020)	Cybersecurity is at the threshold of profound psychosocial impact.
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Michael Charles Hammer, a front-line, supply warehouse manager for UPS
Where do they live?	Brooklyn, NYC

What is the threat?	Someone hacks information in the supply chain to create false demand signals to waste transportation resources and misroute critical supplies. First, the enemy monitors an expensive one of a kind scanner for a port shipping container scanner in the Red Hook Container Shipping facility in the Port of NYC (Brooklyn, NY). This scanner is in a secure, air-gapped network and impossible to access with a traditional hack. However, when the scanner goes down for a critical part (e.g. a infrared camera), the enemy CAN detect the order for this critical repair part and estimate it's routing through the supply chain. Simultneously, the enemy launches a piece of malware in the automated IoT-enabled ordering systems for smart homes and hospitals to cause fake ordering for multiple higher-priority perishable supplies (e.g. baby milk) that will flow along the same supply chain as the scanner's critical infrared camera. This supply chain DDOS malware orders a high volume of higher priority supplies (Dude-- it's BABY MILK) than the camera needed to repair the Port of NYC shipping scanner. To make matters worse, these orders are shipped in and out of NYC using automated cargo trucks putting further stress on the Port of NYC. As the automated cargo trucks are engaged delivering milk, this ends up further delaying the parts neded for the scanner and forces the port to go to manual search and sampling opening the way for a dirty bomb to sneak into NYC.
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
	Mr. Hammer not being able to use a manual override automated system to reroute once the problem has been detected. ("can't touch this"). Red team counts on his inability to override the system, that the shipping of an innocuous product won't directly lead to the actual event (terror attack), and that theport actually lets the nuclear material through. We want Mr. Hammer to have control over the system ("Here comes the Hammer") so they he can prevent the fallout of the cyber-attack on the automated transport control system, which then led to (i.e., prevented) the eventual nuclear attack.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
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?**

	Mr. Hammer detects a spike in several perishable products moving through his supply warehouse. Each of this products is outside the normal levels of demand. This is perceived as a "glitch in the system"
Question Two	**"The Event" - How will your person first hear about or experience the threat?**
	BREAKING NEWS: Severe backlogs in the Port of NYC at Red Hook, Brooklyn are causing major headaches for the Big Apple. Perishable goods in particular are an issue, as hundreds of gallons of milk and baby formula sit on the docks. The issue: Shipping Containers! Local authoritizes are claiming that they can't scan and secure the containers fast enough to keep up with the shipping demand for good flowing into the city. The Mayor is calling for Port Authority and Longshoreman to switch to manual searches to get things back on track.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	**Business Models: What new business models and practices will be in place to enable the threat?**
	Automated ordering in potentially vulnerable smart home devices, integration with automated supply chain.
Question 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?**
	Automated driving ethics clarification and legislation, automated ordering/renewal requirements, privacy protection for sharing/smart devices and appliances. Decreased human oversight of automated systems (increased trust).
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Human on the loop can override automation, and maintain enough human presence and redundancies to be able to switch systems to manual if necessary. For a current case example of how this currently has failed, think that airlines can no longer provide paper tickets or plan flights with a simple computer failure (Delta goes down, August, 2016).
2	Prioritized shipping / distribution lanes (perishables different than high profile goods). Articulated high, medium, and low profile goods for immediate distribution.
3	Smart shipping: integration of transport capacity into automated network. Collective holistic knowledge across network.
4	Alternative scanning techniques
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	Automation Trucks / Shipping & Automated Order Fulfillment. With extensive automation that ties together the shipping and supply industries, they are too integrated to easily override or take down to return to manual ("2 legit 2 quit")
2	Smart Homes/Devices automatically ordering supplies
3	Tipping point where we cannot go back to manual method (corollary to gate point above).
4	
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Build procedures and processes to maintain sufficient human oversight and ability to override/manual each system.
2	Secure transmission of GPS and supply chain information. Resilience against DDOS and ransomware; encryption.
3	Development of secure protocols for IoT systems.
4	
5	

What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Prioritized shipping / distribution lanes (perishables different than high profile goods). Articulated high, medium, and low profile goods for immediate distribution.
2	Integration of transport capacity so that we don't overwhelm shipping throughput. For example, once shipping is saturated, do not backlog the system but hold off shipping until capacity becomes available. This works in conjunction with prioritized shipping above. Analogous to QoS in network traffic.
3	Industrialization of 3D printing, then we'd be able to print the parts directly. We are approximately 10 years away from home-practical 3d printers that can print any replacement part we may need. This would localize the global supply chain and provide needed redunancy.
4	
5	

Threatcasting Worksheet	
Team:	John, Glenn, Erik
Experience Title:	Building the future....literally.
Estimated Date:	2026
Data Points	
Slot #1	We need to think about the people that we think are going to be a threat
Slot #2	Reality Management
Slot #3	Automated decision making
Slot #4	Improve Internet protocols
Slot #5	Emerging tech like robots, 3D printing, IOT
Slot #6	our adversaries have adaptive distributed networks
Slot #7 (It's the year 2020)	Device security rules
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Our person is Frank Caldwell from Detroit, a materials supplier to a General Contractor for industrial construction. He has seen a spike in construction for skyscrapers however the raw material production sources that he used to use have not increased their output. He is concerned about the unknown sources he is getting materials from and the quality of those materials. The builders do not care where the materials come from as long as they can continue to build. There are no laws that regulate the supply chain and quality so he has little faith in the quality of the materials, how the materials are being purchased, and that the money leaving his pocket is supporting unfriendly nations.
Where do they live?	Detroit Michigan
What is the threat?	Unknown market supplying raw materials into the supply chain. Those raw materials may be questionable in quality and there is no way to determine where they are coming from. There may be non-state actors funneling sub-standard materials around trade agreements and creating a "black market" for raw materials which may be supporting terrorism. Frank only uses an automated system to order products, he never talks to a person. The automated system is SUPPOSED to find him only approved products at the lowest price but since the whole system is auotmated, he cannot validate the actual sources as there is no person to talk to. He can fabricate his own steel beams through a 3D printing process but he still procures the raw materials through the same automated system. Additionally, the US raw materials producers and trusted nation producers are seeing a decrease in jobs because the demand for those trusted products keep going down.

Briefly describe how your person experiences the threat.		
	Frank experiences the threat through cheap steel but he cannot verify the origin of the raw materials and quality of that steel. State Dept and Dept of Commerce believe all laws are being followed however standard, trusted sources are being undercut by suppliers of unknown origin.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?		
	Everyone who works for Frank's company and everyone who uses Frank to obtain steel is impacted by suspect steel. The Red Team hopes to use substandard prducts to funnel money into unfriendly nations while at the same time degrading the quality of construction in the US. They are concerned that they may be discovered but the risk is fairly low.	
What is the experience we want the person to have with the threat?		
	We want Frank to find out that the steel is actually coming from a reliable source OR find out where the substandard products are coming from and report the issues to the Dept State or Dept of Commerce who fixes the issue.	
What is the experience we want them to avoid?		
	That Frank continues to operate without understanding the origins of his products and that buildings start to fail at the same unfriendly nation-states or sub-state actors are getting stronger.	
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 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 new capabilities enable the person and their broader community to recover from the threat?		
Question One	**"The Event" - How will your person first hear about or experience the threat?**	
	Frank reads articles in the news that the raw material production in the US and trusted countries has gone down however the demand for buildings and steel related construction keeps increasing. Frank keeps seeing that the unemployment rate for the raw materials producers in the US keeps going up even though the system is supposed to ensure that demand across trusted sources is kept at a constant rate to ensure employment remains constant.	
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?***	

	Frank doesn't actually experience the threat first. A third party, unfriendly nation uses Artificial Intelligence and is able to determine this is going on. The unfriendly nation then is able to take advantage of the automation and issues in the system to destabalize the global economy and at the same time funnel massive amounts of money into their country.	
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?		
Business Models: What new business models and practices will be in place to enable the threat?		
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/local partners must the Red Team team up with?		
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?		
Question One	**Business Models: What new business models and practices will be in place to enable the threat?**	
	A new completely automated global acquisition system is put in place to regulate demand across all couontries designed to ensure employment rates acorss all countries is kept at an agreed upon level and at the same time provide the cheapest raw products for all users. This system has no users that maintain it, it is all machine-to-machine interaction.	
Question Two	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**	
	Artificial Intelligence and machine to machine communications between ordering and supply systems	
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)		
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 Blue Team has control over to disrupt, mitigate and recover from the threat.		
1	Build in a system to validate that the demand/supply matches are within a tolerance for price and supplier	
2	Humans may be required to authoirize transactions until the supply sources can be determined	

	3	Manually create a massive fake requirement to force the unknown supplier to produce beyond his means both to force him/her to identify themselves as well as expend all available resources.	
	4		
	5		
Flags:			
What are the Flags?			
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.			
	1	Someone is massively shorting the market	
	2	Cheap buildings and bridges are being underbid while production of trusted raw products is decreasing. The demand for buildings is increasing, buildings and bridges and vehicles are being produced even faster but the demand for raw materials in trusted countries is decreasing.	
	3	Production facilities are being built by non-state actors or are rapidly being built in unfriendly/untrusted nations such as refineries or factories producing the materials being fed into the automated system.	
	4	Deregulation shipping or transport or any steps in the supply chain. If there is suddenly a push to deregulate how raw materials are shipped or produced.	
	5	A flood of raw materials are available with no increase in trusted nations. This would happen if raw materials suddenly become available at much cheaper rates while the employment rates of trusted producers have gone down.	
Milestones:			
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?			
	1	Cross industry trusted communication required to ensure sources are properly verified. Suppliers and procurement and end users must be required to verify each each other and verify that each piece of the process is happening according to all rules.	
	2	We need a way to automate a "corrupton index" for each of the raw materials industry that is based on a vetted algorithm instead of a best guess method; This would provide a rating indicating the level of corruption for suppliers which would be used as a weight in the automated system.	
	3		
	4		
	5		
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?			
	1	Steel and final product "DNA" testing should occur. As with gold or diamonds, there must be a way to quickly test each product (ie each steel beam) before its use to ensure the composition of the material meets quality control standards. This must happen as quickly as possible so each component can be tested.	
	2	3D Printers have a capability to verify the "trustworthiness" of raw products. As raw materials are introduced into the 3D printer for use in printing, the 3D printer must be able to verify that the components meet some sort of quality control specification. If the quality control is not met, the 3D printer should reject the raw materials and fail to function.	

3	Automated trust system to validate suppliers into the automated system. There must be a way to validate that a supplier is who they say they are and that they are authorized to provide supplies to this automated system. As requests for supplies are aggregated into larger "bundles" (ex. the Army CHESS consolidated buy process), especially acorss countries with different regulations on quality, there needs to be a minimum standard for quality of raw materials that can be verified by anyone providing bids to meet the requirement.	
4		
5		

Threatcasting Worksheet	
Team:	Paul Maxwell, Adam Duby, Rock Stevens
Experience Title:	The Heart of the Sea
Estimated Date:	2026
Data Points	
Slot #1	We need to think about the people that we think are going to be a threat
Slot #2	Manipulation of Social Media (China Gamified CitizenNet)
Slot #3	Automated decision making
Slot #4	Improve Internet protocols
Slot #5	Information Flow
Slot #6	our adversaries are agile and nonstatic, have ability to adapt and develop new capabilities
Slot #7 (It's the year 2020)	A lot hinges on how the political economy of data evolves
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Armando Salazar, owner of several fishing ships ; late 30s, worked his entire life to save up enough money to own his own fleet
Where do they live?	Manila, Philippines
What is the threat?	Chinese intervention attempting to incite border disputes over contested fisheries; social media manipulation, GPS/navigation manip, attacks on distribution centers / loss of shipping manifests, manip of fish market pricing to affect economy
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	

	One of Armando's ships are steered off course due to GPS manipulation and his crew is arrested by Chinese navy; cargo is seized without an opportunity to contest the situation. All 10 fisherman on board are now in Chinese custody; one of which is a newly wed with a son on the way and his favorite cologne is Old Spice because it hids the smell of fish guts. The Chinese are attempting to establish international acknowledgement of their borders and projecting power in the region. The Chinese want to avoid bringing the US Navy into the region or having sanctions placed against them. Armando's other ships no longer wish to sail and he is unsure if he'll be able to make enough profit to cover his monthly margins. He is at risk of losing more ships due to debt collectors and the loss of cargo. Armando was giving the opportunity to recover some items from the ship, one item included a manual tracker of the ship's location based off of celestrial navigation -- leading Armando to believe the GPS' were manipulated. Requires assistance with forensic analysis and assistance from social media giant PlentyofFish for flagging Chinese propaganda.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	**What will the person have to do to access people, services, technology and information they need?**
	Armando will need new fisherman and boats temporarily to backfill his loss; he'll need international diplomats to assist and releasing the imprisoned fisherman; he'll need other fishing companies to use PlentyofFish to assist in providing integrity to the platform, associated data, and outing propaganda/misinformation; GPS integrity; PlentyofFish providing geotagging of where fish were caught with nonrepudiation
Question Two	**What new capabilities enable the person and their broader community to recover from the threat?**
	GPS stability / anti-spoofing devices; nonrepudiation of fishing sites; non-digital alternatives to navigation and the fishing economy
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**
	Nearly all the tech needed to carry out this attack currently exists; the sophistication of the technology would need to improve to prevent attribution to China; China will need anti-anti-spoofing tech to enable this attack
Question Two	**Ecosystem Support: What support is needed? What industry/government/military/local partners must the Red Team team up with?**
	Red Team (China) requires naval support to patrol the area in which the Armando's team was redirected; Propogate international trust; Coorporate with local fisheries to avoid 2nd/3rd order effects of denying trade with Manila based fisheries.
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Nonrepudiation and integrity within GPS platforms; alerts when signals are spoofed. This will prevent the Chinese hackers from steering shipping vessels into contested waters.
2	Invest in backup systems within the economy for improved resilience. If the distribution manifests are wiped clean, the industry needs a way to continue. Restoring backups and operating without digital dependence is critical.
3	Continued international support over open waters -- against China's claim to the seas. Disallowing China to dominate waterways that are critical to other nations' economies.

4	Improved integrity in PlentyofFish -- leverage crowdsourcing for outing bad data points in the system --> big data cannot be relied upon when adversary is injecting data points
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	China building and fielding their own GPS. US currently dominates GPS; China using their own system would enable them to control data at will.
2	International community support for China's territorial claims. If the geopolitical environment changes, the Phillipines may be less likely to withstand this powermove.
3	Health of the oceans limit industry. Fisheries near contested waters become increasingly dangerous.
4	Autonomous systems that fisherman are completely reliant on and cannot override for manual intervention (untrained workers + perishable skills). Automated systems that allow anyone off the street to operate can greatly diminish industry resilience.
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Nonrepudiation and integrity within GPS platforms; alerts when signals are spoofed
2	Invest in backup systems within the economy for improved resilience
3	Continued international support over open waters -- against China's claim to the seas
4	Improved integrity in PlentyofFish -- leverage crowdsourcing for outing bad data points in the system --> big data cannot be relied upon when adversary is injecting data points
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Alternative to GPS that is reliable and cannot be spoofed --> automated computer vision for celestrial navigation
2	National rehearsals of non-digital commerce
3	
4	
5	

Threatcasting Worksheet	
Team:	Mike McDonald, Chris Arney, Chris Claremont
Experience Title:	DetroitX
Estimated Date:	2026+
Data Points	
Slot #1	Beware of your short term bias(s); our brains are not designed to think long-term; we like to think the past is also the future. Our long term thinking might not be as far out as we need it to be; short term thinking gets into the way of long term views so must train ourselves. 1. Understanding/awareness of this weakness; 2. take structured acts to spend time with people with different views (interdisciplinary) to think about the future. Thinking about the future can not be done in isolation.
Slot #2	True Sentinent Beings? True Sentinent Beings will not exhist in 10 years or (probably) even 20; Too brittle to achieve true sentinent standard; But we will be able to do limited cognitive modeling - Manage fear. Leverage goodness. Time to manage risks
Slot #3	Disinformation as a weapons system. Without valid and trusted data, automated systems and data driven systems with human oversight cannot be trusted. This is especially true for social media which has very little way to validate the data via trusted sources. - We need ways to verify data being fed into analytics and automated systems. Machines will routinely be able to pass the Turing Test and we will need to develop systems that can determine whether or not the data being generated is human based AND is valid.
Slot #4	International norms/establish policies that discourage malicious actors. Is CNE acceptable? Does cyber espionage change the spy game?
Slot #5	Supply Chain Ecosystem. Suppliers have suppliers have suppliers. A weak spot in any one of these systems has massive cascading effects on the whole ecosystem. There are national security implications to this, as well. Recent examples include the F-35 breach through subcontractors and Qualcomm chip hardware vulnerabilities, exposing millions of Androids. Sensors to detect and possibly mitigate anomolies in the supply chain
Slot #6	Our adversaries are agile and nonstatic, have ability to adapt and develop new capabilities. Adversaries can switch modes of communication without challenge. Traffic analysis, learn adversary "fist"
Slot #7 (It's the year 2020)	Device security rules. Poor device security continues as firms continue to rush technology solutions to market. - Re-evaluate supply chain management. Ensure that security is critical aspect to technology solutions on the market. Develop a quality assurance program, akin to Underwriters Laboratory or NIST, that informs technology consumers on the security and safety of their technology purchases.
PART ONE: Who is your Person?	

Who is your person and what is their broader community?	Rahim Khan - Teenage son of a high-level tech executive
Where do they live?	DetroitX - Smart City built on the ruins of Old Detroit by a Google-like entity to run an experimental automated Smart City. It's largely populated by and run by this company. It has eclipsed the local government and virtually runs Michigan.
What is the threat?	Cyber->Physical
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
	He IS the threat, unintentionally. He's found a workaround in the smart city to hack the street lights, allowing him and his friends to street race utilizing all green lights, but unintentionally disrupting the "efficiency" of DetroitX. This chain reaction slows down freight trains heading through DetroitX, which must now make up time, and speed up to dangerous speeds.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
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?**
	It's not initially seen as a threat. The kids just want to hack the system to joy ride around. They really think that they're *saving* lives by making the smart traffic lights green for them and red for everyone else, making sure there are no innocent bystanders caught in the race. It's exciting to them, but they don't see what the larger effects of this may be.
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)**

	News of the train crashes will have been made national and international news. The company and the authorities are investigating the train crashes and what caused them. He knows why, but initially wants to hide what he did, but eventually he and his friends come around to help fix the issues.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	**Business Models: What new business models and practices will be in place to enable the threat?**
	The experimental nature of the company, and the city by proxy, enables the threat to take place. Government officials are still technologically illiterate, and therefore cede power to Google, thinking that they must know best. The experimental culture of the company lead to inevitabile defects within the system that can be exploited. Moreover, with DetroitX's success, they want to export it internationally to other struggling cities: BaghdadX, KabulX, DhakaX, JakartaX, SaigonX, Xcetera.
Question Two	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**
	Self-driving cars, smart grids, thinking exponentially about the Audi system that communicates with street lights to count down the time till green, Android Pay/Apple Pay systems, smart clothing/wearables, etc. all integrated to make the most efficient city.
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Find the hackers
2	Find the vulnerabilities that the hackers exploited and patch them
3	Root cause analysis
4	Multifactor authentication to access system
5	Make the system proactive to deter, delay, or deadline anomolous behavior (human input?)
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. This will have a significant affect on the futures you have modeled.	
1	Teenagers - they are virtually uncontrollable and prone to rebel
2	A disempowered local government that *they* themselves has disempowered due to their arrogance. EMS.
3	Outside influencing factors/anomolous behavior that doesn't fit in to the DetroitX efficiency algorithm
4	Integrating personal preferences vs. societal efficiency
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and prepare for recovery from the threat?	
1	They must adjust the algorithm in DetroitX to keep it from becoming a slave to the system (Tokyo train conductors who will derail a train before missing a time hack)
2	Smart cleanup? Smart recovery?
3	Make the system more efficient with buffer areas and allow for variables.
4	If death MUST happen, who dies? IE a car crash - kill the occupants of the car or the errant passerby jaywalking? Who makes that decision - government/company? What happens when the company runs the government?
5	Self-reporting AI that maximize efficiency without human input
What needs to happen in 8 year to disrupt, mitigate and prepare for recovery from the threat?	
1	To export overseas, they must study different cultural, linguistic, and governmental barriers. How does it address terrorism or obstructionist intervention?
2	Must work with local and national governments not just for contracting, but actual input and insight
3	Civil liberties vs. Privacy. Is 1984 less 1984 if it's a company and not the government?
4	New roles for humans to be the ultimate decision makers with AI assistance

5	

Threatcasting Worksheet	
Team:	Bill Cheswick, Dan Huynh
Experience Title:	Logan has a bad day in LA.
Estimated Date:	2026
Data Points	
Slot #1 - 3	Social status is really important and influences more than we assume
Slot #2 - 2	Smart & Trusted Objects (e.g. Smart Shirt)
Slot #3	Misinformation as a weapons system
Slot #4	Investment in security to improve public perception
Slot #5	Emerging tech like robots, 3D printing, IOT
Slot #6	our adversaries have adaptive distributed networks
Slot #7 (It's the year 2020)	Human beings are the center of technology and they are imperfect
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Pharmaceutical salesman - Logan McGuffin, has a new self driving car, spends alot of time on the road visting new clients. Recently moved to LA from Boston. He hates traffic and it has become even worse with the Olymics in town. His new self driving car saves him alot of time on the road and has stored all of the addresses of the places he visits for convenience.
Where do they live?	Anaheim, CA
What is the threat?	A well coordinated terrorist attack at the 2028 Olympics in Los Angeles which involves physical bombs and an a cyber attack on the internet infrastructure. This attack greatly impacts numerous sectors - commercial, government, and military functions. The attackers were radicalized within the US and are US citizens.
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	
What is the experience we want the person to have with the threat?	

What is the experience we want them to avoid?	
	One day at work, Logan's car can't find his client's location; he then tries to call. He pops up his google map app and can't connect to the maps server. There is an internet attack on routers within the US which requires massive physical and on site replacement of hardware. Internet within the US is severly degraded with unreliable estimates of repair times. The effects are too wide spread to be seen. News, public, government, and military functions are impacted to varying degrees. Supply chains are impacted. UPS, FEDEX, and US Postal. Air travel is disrupted. Food deliveries are impacted. 3 Days into the Olympics, there are 3 effective bomb attacks which are being coordinated through a terrorist organization. This organization is the same who launched the internet attack on US routers. The Red team wants to hurt the US econmically and morally through causing chaos and disorder through disrupting the Olympics.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
Question One	**"The Event" - How will your person first hear about or experience the threat?**
	Logan is stuck in traffic. Can't reach his next sales meeting. Is completely lost without his navigation. He has lost touch with his digital world.
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)**
	Bascially he can't. Cell phone, texting, and internet is not functioning reliably.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	

Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
Question One	**Research Pipeline: What technology is available today that can be used to develop the threat? What future technology will be developed?**
	Cyber: Adversary needs to conduct indepth research, testing, and developing of day zero to attack internet router infrastructure. Will need to validate success that exploit works. Will need software and or technology and intelligence to be able to target all the major US routers in the network.
Question Two	**New Practices: What new approaches will be used to bring about your threat and how will the Red Team enlist the help of the broader community?**
	Combination of attacking legacy hardware to bring about effect with a physical attack of explosives.
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Actively push hardening of back bone routers of US internet infrastructure
2	Improve relationships and information sharing across private and government parties involved with internet infrastructure - promote flexibilty and agility to react
3	Improve monitoring of dark web and open source research of these attack types
4	
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	day zero attacks on routers and other key internet infrastructure equipment

2	increased radicalized lone wolves
3	
4	
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and prepare for recovery from the threat?	
1	working with router manufacturers to better understand threats, vulnerabilities, and recovery
2	develop and employ a system for tracking and identifying internet mapping work
3	run feasibility tests on attacking internet infrastructure routers
4	
5	
What needs to happen in 8 year to disrupt, mitigate and prepare for recovery from the threat?	
1	employ standards for routers on government hardware to help push commercial sector usage
2	
3	
4	
5	

Threatcasting Worksheet	
Team:	
Experience Title:	Infernal Combustion
Estimated Date:	2026
Data Points	
Slot #1	Human self-protection system (classical vs behavioral); we have both systems in our body but our cyber systems are only designed one way
Slot #2	True Sentinent Beings?
Slot #3	Micro-Targeting
Slot #4	Need better info campaigns for defeating hacks and defending networks
Slot #5	Emerging tech like robots, 3D printing, IOT
Slot #6	Asymmetric adversary attacking soft targets
Slot #7 (It's the year 2020)	Cybersecurity is at the threshold of profound psychosocial impact.
PART ONE: Who is your Person?	
Who is your person and what is their broader community?	Joe Shmoe - Boogle self driving car project CTO and tech lead.
Where do they live?	Palo Alto, CA
What is the threat?	The adversary wishes to compromise the control code and systems of the self driving car project that allows cars to operate autonomously on the highways in coordination with other autonomous vehicles. The plan is to inject malicious code into the fail-safe systems and allow remote override. The adversary's intent is to cause mass casualities, infrastructure damage and reduce the confidence in automated technologies. The plan is to override as many vehicles as possible during commute hours nationwide on highways and inside tunnels.
Briefly describe how your person experiences the threat.	
What is it? Who else in the person's life is involved? What does the Red Team want to achieve? What is the Red Team hoping for? What is the Red Team frightened of?	

	By creating this catastrophe, the adversary seeks to destabilize US society and strike another symbolic blow against the US homeland. An additional goal is to cause another massive financial expenditure of national treasury to weaken the US economically. The event could also be used to distract the US from responding to other aggressive behavior by nation states elsewhere around the globe by consuming time and resources locally. The adversary will be concerned with being identified and the potential for a massive reataliatory response by the US.
What is the experience we want the person to have with the threat?	
What is the experience we want them to avoid?	
	Shmoe is attending the international auto show in Geneva to promote the latest model of the Google self driving car. He goes to dinner and leaves his corporate laptop in his hotel room. Agents from an unidentified adversary gain access to the hotel room and compromise his laptop. This provides remote access and control after he returns to the US.
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 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 new capabilities enable the person and their broader community to recover from the threat?	
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?***
	Vehicles will begin driving erratically, increasing speed and changing lanes at random. City agencies responsible for traffic control will be unable to determine the cause and unable to react before the incident reaches catastrophic proportions. The ability of the military to mobilize in response to the threat will be adversely impacted by accidents outside of military installations.
Question Two	***What new capabilities enable the person and their broader community to recover from the threat?***
	Nationwide halt to all autonomous vehicle operations with the exception of emergency response units. Immediate code review by all vehicle manufacturers to determine whether or not the issue was intentional or accidental. Development of new "fail-safe" technology to ensure safe operation in the future.
PART THREE: Enabling Questions - Red Team (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 Red Team enlist the help of the broader community?	
Business Models: What new business models and practices will be in place to enable the threat?	
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/local partners must the Red Team team up with?	
Training and Outreach: What training is necessary to enable the threat? How will the Red Team educate others about the possible effects of the threat? And how to bring about the threat?	
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?***
	Physical access to the target laptop. Remote access once Urmson returns to the US. Lateral movement within Google's network. Privilege escalation and access to relevant code-bases. Expertise in autonomous vehicle systems and code design. C2 access to traffic control systems that integrate with autonomous vehicles.
Question Two	***Ecosystem Support: What support is needed? What industry/government/military/local partners must the Red Team team up with?***
	Financial support, guidance, and technology. Intel to assist in targeting and code development. These can be provided by private sector companies and/or government agencies of US trade partners (e.g. China, Russian, North Korea).
PART FOUR– Backcasting - Blue Team (from the perspective of U.S. Forces)	
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 Blue Team has control over to disrupt, mitigate and recover from the threat.	
1	Maintain physical security of electronic devices when traveling. Use burner devices for international travel.
2	Ensure secure coding practices are utilized. Code reviews are completed in a thorough manner prior to production release.
3	Create a government controlled "all stop" fail-safe mechanism to disable autonomous vehicles in a controlled fashion.

4	Require on-board override of autonomous systems. Driver taking control.
5	
Flags:	
What are the Flags?	
List out what the Blue Team doesn't have control over to disrupt, mitigate and recover from the threat. but this will have a significant affect on the futures you have modeled.	
1	There will always be those who attempt to find weakenesses in technology systems.
2	Autonomous vehicles are coming. As they become more prevalent the risk of this type of attack increases
3	As long as humans are part of the development process, mistakes and coding errors will be made. This allows an adversary to gain access and conduct malicious activity.
4	Once an event takes place, there is limited ability to control the immediate outcome and impact.
5	
Milestones:	
What needs to happen in 4 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Establish industry standards for security and coding when developing autonomous vehicle systems.
2	
3	
4	
5	
What needs to happen in 8 year to disrupt, mitigate and perpare for recovery from the threat?	
1	Standarized, international safety certification process is developed to ensure proper operation of autonomous vehicles.
2	Create segregated travel lanes/pathways dedicated to autonomous vehicles.
3	
4	
5	

Research Synthesis Workbooks

Research Synthesis Worksheet				
Slot:	Group 1 (Awesomeness)			
Group Members	Julia Rose West, Andy Hall, Natalie Vanatta			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	There is no one general system to detect threats and opportunities; our minds are not developed to do deep thinking so we need time to think through things	qualitatively distinct systems; designed to fit different niches; there are not created with the idea to interconnect; our systems have to have time to work through things	Negative (harder to secure it all especially the interconnections); Positive (mitigates risk if one goes down; learn from one system getting attacked; have all senses engaged)	need to view the system as a system of systems; should not try to create one omega system; focus sub-systems on one thing they can do well; acknowledge that systems are looking at different things and have strengths/weakness in each
2	Human self-protection system (classical vs behavioral); we have both systems in our body but our cyber systems are only designed one way	re-think how we design cybersecurity threat detection systems to work like a behavioral immune system (lower cost, better results); cost is on me but benefit to ; not enough real time learning in the systems to benefit the individual	Positive (two different types of thinking makes the system stronger) ; Negative (would be that to a system that anticipates - is the false anticipation)	use systems that complement each other ... some that work in the classical way and some that are behavioral in order to better ape what the human body does
3	Social status is really important and influences more than we assume	status indicator in social media is size of your network but the larger the network the lower your security posture; so as we crave more status - we get weaker	Negative	famous people have to use different protection mechanisms (physical) than normal folks; we need to adapt that idea to the cyber domain also - an understanding in the populace; another idea is that the most popular person in the network should be lookign at the least popular person as a source of valid information (creating trust categories, scores, and relationships)
4	We need to think about the people that we think are going to be a threat	intelligence gathering is a key piece to cybersecurity; which means that there is some collection on US persons; globaliness of cyber persona; we have to be able to understand other people and cultures also	Positive and Negative	Movies where we arrest people before the crime. THe danger is that we create that as our future. We must know our adversaries like Sun Su said but limits need to be created.

5	Beware of your short term bias(s); our brains are not designed to think long-term; we like to think the past is also the future	our long term thinking might not be as far out as we need it to be; short term thinking gets into the way of longterm view so must train ourselves	Negative (cuz stuck in a rut)	1. Understanding/ Awareness of this weakness; 2. take structured acts to spend time with people with different views (interdisciplinary) to think about the future. THinking about the future can not be done in isolation.
6	Many of our cues we inately use are from our evolutionary past; evolutionary cues and environmental cues	we could take cues from older technology that influence us; age of population and age of technology - as we go forward different ages of the population will respond to different environmental cues differently ... ultimately that can be used against them by attackers; (also, combining the idea of postal mail and telephone to come up with an explanation of email)	Negative	WE should be able to tune our protection to our experience and our beliefs in our own cues. So if I know email, but I want to try something new - then I should be able to put it in the most protected status until I understand the tech better and can understand/recognize the cues that work for the new tech vice what worked for my past understanding of tech. ((Think about how we handle children with cognitive disabilities ... that we have more parental control of cues until they understand them.))
7	Smoke Detector Principle - we assess risk and then calibrate our tools/lives to minimize risk rather than maximize happiness	false alarms and missed alarms ... the balance between the two	Positive (the principle is because it helps us identify the end points) ... the implications could be negative; technically by calibrating could be positive also especially if creating a learning system	When calibrating the system, if we tune it for threat detection then we need to screen what comes through for opportunities. If we calibrate to detect opportunities, then need to screen what comes through for threats.
8	Context affects perception;	how vulnerable you feel is based on other threats in your environment; some situations you would be hyper-vigilent but you can't always be (change in your posture based on whether at work than home)	Negative	A certain amount of vulnerability is good. If you are aware of this, you could be stronger. You could have time-based, filtering of threats so when you are in a situation that you are least secure - that your protection is better. I.e. you are on a metro from 4-6am and you know you are just clicking on things to kill time, then you can turn up your protection to only allow really good things through the defensive posture because your situational awareness is low.
9	opportunity management systems are the other side of the coin to threat management systems;	looking for opportunities, cues for opportunities, and how we make decisions about opportunities might take same or different information than the threat ; there is a marketing target based on opportunities that are threats	??	When calibrating the system, if we tune it for threat detection then we need to screen what comes through for opportunities. If we calibrate to detect opportunities, then need to screen what comes through for threats.

Research Synthesis Worksheet				
Slot: 2	Rise of Sentinent Machines			
Group Members	Ali, Rob, Fernando, John, Steve		Person in situation solving problem	
#	Data Point	Implication	Positive or Negative?	What should we do?
1	True Sentinent Beings?	True Sentinent Beings will not exhist in 10 years or (probably) even 20; Too brittle to achieve true sentinent standard; But we will be able to do limited cognitive modeling	Positive	Manage fear. Leverage goodness. Time to manage risks
6	Smart & Trusted Objects (e.g. Smart Shirt)	Data is no longer hosted; Data lives among an infinite set of networked devices; Data is never at rest; person can grab data anywhere; IoT broadcast massive amounts of data	Both; Apparel scenario...Positive (Medical applications of appearl) Negative (Wardrobe malfunction)	Establish trust
7	Reality Management	Mass amounts of data; We start gisting vs. exacting. Realtime simulation on your hip will mean you can preevaluate everything and all outcomes	Positive (human adaptation to pervasivice hyperlocal, unreliable data)	Establish trust
8	Commanding Data & App Creation	Autonomous devices will generate data and do things on their own. Apps are being generated autonomously by large platforms. How do we control these? Corporoate entities will command platform, we will suscbribe to effects	Positive	Establish control via infrastructure
9	Manipulation of Social Media (China Gamified CitizenNet)	Social media apps being used to create gang behavior or controlled citizens	Negative	
10	Living off the Grid	How can one opt out of capabiltities and social norms created by technology? Should they be allowed to?	Negative (will create divergent behaviors)	

Research Synthesis Worksheet				
Slot:	Miss Information			
Group Members	Erik Dean, Glen Robertson, Clint Watts			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Micro-Targeting	Ability to provide better targeting data to limit impact to bystanders. We will have to emply much better deceptive techniques to provide cover for agents and leaders which is significantly harder to do.	Both	Legislation would need to be created at different levels, national security, third party / business, law enforcement. External countries may require additional restrictions such as only storing microtargeting data in the country of origin of the person. Privacy concerns and rules in different countries are different which may cause issues.
2	Automated decision making	Human assisted automated solutions for transportation (navigation, traffic, finding parking, aviation safety) healthcare (diagnosis, treatment, trauma care)	mostly positive	Use algorithms to help us make better decisions and know when or when NOT to override the system (avionics example)
3	Misinformation as a weapons system	Without valid and trusted data, automated systems and data driven systems with human oversight cannot be trusted. This is especially true for social media which has very little way to validate the data via trusted sources.	Both	We need ways to verify data being fed into analytics and automated systems. Machines will routinateely be able to pass the Turing Test and we will need to develop systems that can determine whether or not the data being generated is human based AND is valid.

Research Synthesis Worksheet					
Slot:					
Group Members	Paul Maxwell, Rock Stevens, Adam Duby				
#	Data Point	Implication	Positive or Negative?	What should we do?	Category
1	Improve Internet protocols	Internet is too well established to start anew; new protocols and new delivery mechanisms will support security and privacy desires	Positive	QUIC, IPv6	
2	Engineering practices	Cross-discipline approach to improving network-connected systems	Positive	Explicity state security requirements upfront	
3	Investment in security to improve public perception	Change the "swordfish" black hoodie, basement hacker perception of hackers	Positive	K-12 security awareness programs; bug bounties; mentors for asipring professionals; professionalize the careerfield	Public awareness / education
4	International norms for self-securing	Make it easier for people to defend themselves	Positive; establish the baseline that others CAN exceed if desired	"Fire station child seat checks" for cybersecurity	Public awareness / education
5	Professional licensing for developers	Matching requirements for development with impact on society	Both; added overhead and stifling creativity but upping requirement for people that place our data at risk	state / fed certifications	
6	Need better info campaigns for defeating hacks and defending networks	let the population know that cybersecurity DOES work	Both; IGL	publishing success stories better; phase out fear; educate that it's not like the movies	Public awareness / education
7	International norms / establish policies that discourage malicious actors	Is CNE acceptable? Does cyber espionage change the spy game?	Both; loss of offensive power		

Research Synthesis Worksheet				
Slot:				
Group Members	Mike McDonald, Chris Arney, Chris Claremont			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	60% of all cyber attacks are all originated from trading partners or criminals seeking to exploit vulnerabilities in the supply chain	Degraded trust between trading partners. Are the trading partners empoying criminals? To what end?	Negative	Cease trade with trading partners and look for/form new partnerships
2	Emerging tech like robots, 3D printing, IOT	Supply chain entities may fight against each other for a competitive advantage. Increased efficiency in the system = reduced cost	Negative/Positive	Government action on behalf of private corporate entities
3	Information Flow	If you disrupt enough just to delay the supply chain, it may have exponential implications in delivering a product to the customer, breaking the trust.	Negative	The information and product flow must be protected in the highest manner
4	Supply Chain Ecosystem	Suppliers have suppliers have suppliers. A weak spot in any one of these systems has massive cascading effects on the whole ecosystem. There are national security implications to this, as well. Recent examples include the F-35 breach through subcontractors and Qualcomm chip hardware vulnerabilities, exposing millions of Androids.	Negative	Sensors to detect and possibly mitigate anomolies in the supply chain

Research Synthesis Worksheet				
Slot:				
Group Members	Bill Cheswick, Dan Huynh, Carlos Vega			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	our adversaries are digital natives	defenders need to also be digital natives, must be able to defend from multiple avenues, must be agile and adaptive	Negative - our adversaries can be more agile than us	build / foster edge organizations who have autonomy and authority to operate to accomplish their missions; must be willing to innovate
2	our adversaries have unprecedented knowledge of our TTPs	adversaries can easily identify our equipment and personnnel security vulnerabilities, patterns, and MO and exploit them,information disclosure, messaging,	Negative - we lose a perceived advantage	commander's intent; better opsec; introduce unpredictability; **heisenberg management**
3	our adversaries have adaptive distributed networks	adversaries are hard to pinpoint - edges and centers of gravity, difficult to impact	Negative - hard for us to combat	micro-targeting, network isolation, network shunning, introducing counter message into their network
4	our adversaries are agile and nonstatic, have ability to adapt and develop new capabilities	adversaries can switch modes of communication without challenge	Negative - hard to keep up	traffic analysis, learn adversary "fist"
5	Asymmetric adversary attacking soft targets	Target families and loved one to impact the will to fight	Negative - non standard, unprepared to defend	teach the new normative behavior and provide protection on all fronts. **Protect the Social Supply Chain and Social Capital.**

Research Synthesis Worksheet				
Slot:				
Group Members	Brian Schultz, Sean Griffin, Rhett Hernandez, Gus Rodriguez			
#	Data Point	Implication	Positive or Negative?	What should we do?
1	Human beings are the center of technology - and they are imperfect	We cannot fully remove the risk inherent to human beings within the operation and development of a system.	Negative	Continue to efforts to minimize and reduce exposure to that threat vector as much as possible -whether that is redundant code checks or user education.
2	Hackers go mainstream	Hacking will no longer be considered a special skillset and thus digital crime will increase. Assets will be at more and more risk.	Negative	We cannot stop people from learning more about technology. Local law enforcement will have to increase technical education and adapt to changes in the crime landscape.
3	A lot hinges on how the political economy of data evolves	Criminals continue undertaking increasing large breaches in order to build treasure troves of data that can be sold, used, or bartered with at a later date.	Negative	Encourage society to treat data as valuable and protection as much as their personal possessions.
4	Device security rules	Poor device security continues as firms continue to rush technology solutions to market.	Negative	Re-evaluate supply chain management. Ensure that security is critical aspect to technology solutions on the market. Develop a quality assurance program, akin to Underwriters Laboratory or NIST, that informs technology consumers on the security and safety of their technology purchases.
5	Cybersecurity is at the threshold of profound psychosocial impact.	Cyber Security's impact on the public physcology erodes trust in the financial and other systems that form the building blocks of modern society.	Negative	Education and public/private partnerships that encourages shared responsibility in our collective security.