Safeguarding Critical System Supply Chains Against Compromise Workshop
July 14, 2022

University of Maryland

MChESS

Maryland Center of Excellence for Sustainment Sciences

calce

Funding for this project was provided by the National Science Foundation Division of Civil, Mechanical and Manufacturing Innovation (Grant No. CMMI2039958)

Safeguarding Critical System Supply Chains Against Compromise Workshop

"Critical systems" are systems associated with human safety (transportation, medical), the delivery of critical services (infrastructure, energy generation), important humanitarian and military missions, and global economic stability. The risk of supply chains being compromised is a significant problem for critical systems due to the system's long manufacturing and support life. Compromise of a system *component* means that its content, function, quality and/or reliability has been modified in some way (either with, or without malicious intent) to be something other than what the system expected (i.e., was qualified for).

The supply chains for system *components* can be compromised by natural events or the active introduction of manipulated parts, materials, software, or information, as well as interferences with networks and processes.

Sourcing *components* for critical systems is a challenge because the supply chains for the *components* diverge from mainstream commercial supply chains over time. As a result, the operators of critical systems impose a myriad of restrictions on how *components* can be sourced in order to minimize the risk of compromised *components* finding their way into critical systems. Similarly, the information that these systems depend on to operate can be compromised impacting the system's support and/or manufacturing. These requirements limit the available sources and can make the process time consuming and expensive and on the other hand open opportunities for impostors to enter the supply chain.

This workshop focused on the unique issues posed by compromised *components* (hardware, material, software, data, algorithms, humans), and how they can be predicted and mitigated. This is a convergent workshop whose participants will include academics, industry practitioners, and stakeholders from the critical systems community whose concern is disruption and compromise of the technology and supply chain for critical systems. The workshop addressed the following topics:

- Morning Keynote: An Argument for a Systems Approach to Supply Chain Security
  - Christopher Nissen (ARLIS)

- Blockchain for Supply Chain
  - Ujjwal Guin (Auburn) – Panel Chair
  - Hale Summers (Sikorsky) - Panelist
  - Radu Diaconescu (Swissmic SA) – Panelist (virtual)
  - Harvey Reed (MITRE) – Panelist (virtual)

- Trust
  - Jeremy Muldavin (GSA TIES and GlobalFoundaries) – Panel Chair
  - Candace Moix (START) – Panelist (virtual)
  - Eileen Dombrowski (GlobalFoundaries) – Panelist
  - Sylvere Krima (NIST) - Panelist

- Afternoon Keynote: Risk, Threat, Vulnerability, Consequence
  - Bill Stephens (ARLIS)

- Human Aspects of Compromise
  - Steve Sin (START) – Panel Chair
  - Bill Stephens (ARLIS) - Panelist
  - Anthony (Tony) Kraemer (Cape Fox Shared Services) - Panelist
  - Juliet Aiken (Conducere) - Panelist

- Public and Organizational Policies
    - Charlie Harry (UMD) – Panel Chair
    - Bruce Kaplan (LMI) – Panelist
    - TJ Zitkevitz (Lockheed Martin) – Panelist
    - Kirsten Koepsel (McKinsey and Company) – Panelist (virtual)

- Modeling, Analytics and Data
    - Tim Sprock (ARLIS) – Panel Chair
    - Neil Brock (Draper) – Panelist
    - Peter Sandborn (CALCE, UMD) – Panelist

The workshop was held in-person at START (National Consortium for the Study of Terrorism and Reponses to Terrorism) had 42 participants (38 in person and 4 virtual panelists). The workshop was recorded to assist in the production of this report (the recording was destroyed after the preparation of this report).

Organization of this Document

This document provides an overall workshop summary followed by summaries of the individual panels. This document follows the Chatham House Rule with redaction of individual names and organizational identifications.

Workshop Summary and Outlook

Peter Sandborn (Engineering, University of Maryland)

This workshop was an attempt to consolidate several different aspects of the supply-chain compromise problem, but was by no means a comprehensive treatment of the issues at hand.

Supply chains are commonly defined as the network between a company and its suppliers used to produce, distribute and sustain a specific product or system. The supply chain can also represent the sequence of steps necessary to combine or transform a set of components into a system for the customer (and then continue to support that system during its useful life). This network includes many different activities, people, organizations, information, and resources. The common perception of a supply chain confines it to just "produce and distribute", i.e., often omitting "sustain", but for critical systems, supply-chain management is potentially more challenging in the sustainment phase of the system's life cycle. Although the term "supply chain" infers a linear or serial system in which each tier only has one supplier, for most systems the supply chain is really a complex network consisting of many nodes and edges.

For critical systems, supply chains represent a key element for insuring system resiliency. Resilience is the intrinsic ability of a system to resist disturbances or the ability of the system to provide its required capability in the face of adversity. True system resilience requires that a system to be reliable (i.e., hardware and software that doesn't fail), and be supported by logistics, contracts, governance, business model, and workforce that also doesn't fail or disappear. The supply chain obviously represents a point of failure for a system. An operator (or customer) has to be able to source the system's components in both a dependable and secure way for as long as the system is sustained.

The relevant definition of compromise in the supply chain world is "to cause the impairment of". Compromises of components and their supply chains can be the result of intentional actions (malicious intent) or the result of a myriad of unintentional circumstances. This workshop discussed compromise from the following distinct points of view:

> **Supply-Chain Trust**, fundamentally this is a confidence metric that humans assign. Trust is situational and evolving. Blockchain for supply chain is one method that has been suggested for establishing trust. Human (workforce) is another vector of trust and policy is a mechanism that creates rules and guidelines that codify assurance (the actions one takes to ensure trust).
>
> **Supply-Chain Security** views the supply chain as a threat environment that potential adversaries can take advantage of (i.e., the supply chain can be viewed as an asymmetric weapon where a relatively tiny effort can potentially create a large return for an adversary).

Security is the state of being protected or safe from harm, and represents a key component for establishing trust within a system. Both security and trust are necessary for a system to be successful in performing and continuing to perform its mission throughout its life cycle.

The sections that follow explore the intersection of trust and compromise.

Summary of the Blockchain for Supply Chain Panel

Thomas Hedberg (ARLIS, University of Maryland)

A blockchain is a type of distributed ledger technology that consists of a growing list of records, called *blocks*, that are securely linked together. Each block contains information about the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed when the block was created. Since each block contains information about the previous block, they effectively form a *chain*, with each additional block linking to the ones before it. Consequently, blockchain transactions are irreversible in that, once they are recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks. Blockchain concepts applied to the supply chain may provide a way to detect compromised products in the supply chain.

Exercise: The people in the room could actually create a blockchain right now, they could take their pens, and they could take a piece of paper and they could start passing around a bottle of water, and everybody just takes notes about the path that the water bottle takes: Person A transmitted the bottle to person B etc., and then we vote, and we agree that person A gave the bottle to person B and so on. Everyone's notes are their version of the ledger. This is fine until someone in the back of the room decides that person A didn't send the bottle of water to person B, they sent it to person C instead. Now when we vote, we couldn't reach consensus.

This panel discussed several aspects of the application of blockchain to supply chains.

Traceability - the quality of a system or subsystem having an origin and a path from that origin to its current state.

- Complexity of products and complexity of their supply chains (hardware and software) make traceability a challenge.
- There are various traceability solutions and no one traceability solution will win out (we have to make sure that data is not lost across the value chain) through the standard and through techniques like zero-knowledge proofs or verifiable credentials, and using the blockchain, we can construct a product identification process.
- Each sub-assembly's providence data has to be attached to it, so that whenever we deconstruct a product we have access to it.
- The good news with blockchain is it's public it's chronological (i.e., time stamped), and it's traceable. There's traceability with the transparency.

Security – how can an adversary attack the blockchain?

- How we're going to make sure that, if we implement blockchain and created a decentralized ledger. How are you going to address the security? Not only in the software but also the human part?
- To take over and you'd have to wipe out a whole bunch of nodes by the time those attacks are underway.
- People, you know, if you're doing high chain you know people could be alerted and then take mitigation steps.
- Most of the blockchain discussion would be a well-defined set of people operating a well-defined, set of nodes, and then hopefully applying very good security practices.

Zero-Knowledge Proof - A zero knowledge proof is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.

- Not all applications need blockchain. Most of them can just use an ERP or some companies can use a shared ERP system that's perfectly fine. But if we decide to leverage blockchain, then there needs to be a reason for it.
- If we are going to use blockchain in the context of supply chain, we require zero knowledge proof.
- Supply chain actors want to keep as much as possible secret sensitive, even you know who they're sourcing from secret sauce, and they house that data in their proprietary ERP systems.
- As a vendor, if my data is open, i.e., if I put everything on the chain, then then there is no competitive advantage for me. So how does a vendor of a part provide a zero-knowledge proof to their customer? The whole community needs to decide. What do we want to see? and how do we want to participate?
- The community needs to decide (agree) on what should be shared? What is the common language for sharing the information.
- One of the biggest misconceptions is that all the data is public. It's true to a certain extent but it's an inherent property of public blockchains, but this doesn't mean that all the data has to be public.

Truth –

- What truth do people expect to be on the blockchain?
- There is no a 100% truth. It’s just what was recorded.
- Blockchain does not prevent anything. It only makes what has occurred obvious.
- Blockchain itself is not a detection technique. It is a method of assigning blame.
    - Blockchain allows anomalies to be in trace it back to the point of ingress. The sole purpose of using blockchain in the supply chain is being able to figure out what went wrong.
    - This doesn't mean that the point of ingress will be a 100% responsible for an anomaly.

Summary of the Trust Panel

Diganta Das (Engineering, University of Maryland)

One commonly used definition of trust is the confidence that the system will behave as intended, free of defects and vulnerabilities over the system's lifetime. It is a confidence assurance method with a set of actions to instill that confidence or trust. In this manner, zero-trust is a subset of trust. It ensures confidence in the system by utilizing a multi-factor provenance and traceability before an entity is given access to all the keys and the ability to enter, maintain, or alter any system. Thus, zero-trust is an assurance principle that installs trust. The elements of trust are confidentiality, integrity, and availability of the system in the supply chain.

While the definitions above apply to all products, this panel discussed trust in the context of microelectronics. Microelectronics has an incredibly complicated distributed supply chain with very complex technology and manufacturing processes (complex and precise equipment working at the edge of physics builds microelectronics).

The panel considered how research and development contribute to building confidence, which needs to be matched with related economic capabilities (economic decisions are integral). One goal is to decide how to spend resources contributing to a production advantage around these critical sectors. These decisions also relate to building boundaries that protect national interests. Other nations are offering economic incentives; the US needs to build such boundaries with market incentives to make it sustainable. The panelists were posed with the following open-ended questions:

- What is their view of the problem around trust?
- What is the real thing that we have to trust?
- What are the most critical parts of that problem?

The cost of implementation of trust across the supply chain is high. The supply chain consists of large and small companies, with most members being small. Small companies find it hard to invest in a new process, however, these companies are equally crucial to the supply chain and need a support structure to enable them.

All supply chains include consumers, and they can become the sources of vulnerabilities. The consumers may bear the brunt of a lapse in trust, but they may not understand or be willing to participate in managing it. Trust needs to be framed in a way so that the consumer sees value. Consumer participation and buy-in are needed to build trust and demand trust. Even if the system is trusted, resilient, and reliable, the system will have a reputational problem in the market if the end users don't trust it. The Colonial pipeline ransomware attack created market panic even though the direct impact on the petroleum supply was limited. One has to secure the hardware and work on "like" public messaging to make sure that consumers trust the process.

An international supply chain is a norm for all microelectronics. On average, 25 countries are involved from conceptualization to marketing. The members of this supply chain must trust sharing data with theirs partners and the material they receive from their partners. Only about five pure-play foundries are involved with most critical microcircuit fabrication. For them to be trusted, there must be validation of several factors, such as not overproducing and not producing using stolen intellectual practice. They need to show compliance before gaining access to partner activities. They also need to show that they can identify and stop the proliferation of IP that they receive.

Trust can change with time as the systems are updated and modernized. The trust system requires quick turnarounds to match the updates. One concern is that many organizations are unsure how to inventory or assess their internal assets. As a result, these organizations don’t always even know how to secure their infrastructure.

Adversaries can inject themselves into supply chains, and attack managed service providers, people who have access to sensitive data, or the government. Just the possibility of this scenario is enough to deteriorate trust. It doesn’t matter if that hardware is trusted and reliable if public sentiment doesn’t reflect that, e.g., the public’s perception that there are problems with items such as trust in voting machines and election integrity. An organization must ensure that its customers know where products are coming from and that they are trusted. The cost of inaction could be widespread for society.

Everybody must understand the customer across the supply chain of hardware, firmware, software, and suppliers. In each of these steps, the consumer or user can be at risk or be a source of risk. With connectivity across the products, the impact could be catastrophic. Connected vehicles could become weapons on wheels, and smart cities can become disrupted through various utility systems such as the electric grid, telephone, and water supply. Every IoT device can be hijacked or can provide false information. However, the marketplace is often unwilling to pay the premium for insurance against disruptions, and more secure products may lose out in the marketplace. Security-conscious acquisition professionals cannot solve the problems unless the consumers are on board. In many organizations, a component of awareness is the monetary quantification of trust. How does one value confidence in the supply chain, which may be invisible or unknown? How do you get organizations to buy into something a bit more secure? We are concerned about availability. Everyone knows what happens when you can’t get critical manufacturing goods into your supply.

What does success look like in building and maintaining trust? It is best not to be complacent and have a false sense of security. While one can take small steps and validate the impact of those steps, an organization and the supply chain may never get there. Trust is never at 100%. Success is ensuring we are always trying to improve and keep improving. Success looks like being aware of the challenges of having a risk, or the valuation of the risk, and being able to continue. One must make decisions and take action to protect their organization, continually with awareness and the ability to benefit from a more shared system. Success is reducing the vectors of attack and the number of incidents that do occur. Winning is developing an environment where companies understand the imperative of making investments in this domain and continually strengthen security for a layered defense and depth approach. One can reduce the attack vectors and promote a version of self-regulation and enforcement. Analogous to traffic enforcement, where there are first signals and then enforcement, one can ask the partners to put safety mechanisms like logic or PUF and “penalize” them if they fail to do so. In this connected system, the concept of winning has to evolve.

From a consumer’s point of view, they are not persuaded by technology, but by brand, and the brand has to build that trust over time. There can be reputation management for companies, but at times of scarcity, the best practices can be abandoned, and the reputation can be quickly lost.

Another view of success (or progress) is to increase the cost for the adversary. If appropriate technology barriers are in place, the adversary will be forced to develop human assets that are easier to protect against and intercept. Security against human assets is often accomplished using the “guns, guards, gates, background check clearances, provenance.” approach.

While many companies are comfortable looking at their software systems and assessing them for trust, it is uncommon for people to think how hardware could be the problem. At the semiconductor level, there is a need for proper accreditors, trusted foundries, and access to them in a guaranteed manner. Punishment has limited utility in public policy, and methods like debarment cannot be used forever. The industry welcomes government investment and incentives. Groups like GSA-TIES wants the government to support observability and traceability, reporting securely, and financial incentives in the form of taxes and loans. Government can make tax policies creating incentives or provide loans at a lower rate to incentivize companies to value trust more. The government can make important policy decisions to make investments about what, where to build plants, where to build foundries, how to ensure technology, and what requirements of carrots and sticks to use.

Several policy tools available – both immediate and long-term that would require an act of Congress that could be utilized to create a shift in attitude to value security. It can install stability requirements as a condition of Federal funds by requiring visibility into the supply chain and where the various risks are. They can require supply chain and operational security standards for using critical infrastructure. These can inform policies for national security. As a result, such a supply chain can have a system where a manufacturer is integrated into the more distributed supply chain.

Summary of the Human Aspects of Compromise Panel
Marcus Boyd (START, University of Maryland)

The Human Aspects of Compromise Panel covered focused mainly on the industrial psychology behind why humans decide to commit breaches of trust in the workplace. The panel chair and one of the discussants are experts in the field of counterintelligence and insider threat risk and vulnerability. The two other discussants are both experts in the field of industrial psychology and have significant academic and professional experience investigating trust, safety, and compromise.

- Fallibility of Humans
    - Humans are the weakest link of any secure environment.
        - Humans are vulnerable to various forms and types of influence
    - Malicious intent is often assumed when a compromise event occurs
        - This is often the case, but not always
        - An individual may act out of grievance or carelessness
- Securing a Workplace:
    - There are two routes to insecure workplaces:
        - Carelessness
        - Grievance
- Culture and Climate of Workplaces
    - Leaders and leadership define culture and climate
    - Culture is what is valued and what matters within a workplace
        - This is a messy concept and unclear definition within industrial/organizational psychology, but boils down to the way we see culture at work
            - Office doors open or closed tell you about the person behind the door
    - A key concept within a workplace's culture is what behaviors, events, etc. are rewarded?
        - Climate can be for a specific goal/purpose
    - To make a workplace more secure, foster a climate of security and safety
        - Ensure that policies are oriented toward safety and information security
        - Ensure policies are written so new employees understand expectations
    - Climate is shared
        - Employees need to have a similar understanding of expectations
            - If they do not agree on climate, the result is a mess
            - Need agreement and clarity on policies, expectations, procedures
            - Need consistent enforcement of violations
            - Need accountability
                - If people are not accountable, policies are meaningless
        - Organizations that lack a shared climate suffer
            - Leaders, managers, and staff are uncomfortable explaining concerns
            - Avoid difficult conversations
- Organizational Considerations
    - Compliance functions – these need to be truly independent
        - Needs to be at a level within the hierarchy of an organization that it can operate without conflicts
    - Staffing structures

  - Determine the ideal staffing structure to prevent a bad actor (or bad hire) from causing too much damage
    - This means oversight, empowered managers, and staff that feel comfortable sharing concerns

- Leadership
  - *People do not lead organizations, they lead their leaders*
  - Many styles of leadership
    - Toxic leadership has a negative impact on the organization
      - A leader who is really focused on their own objectives
      - They self-promote
      - Develop asymmetrical relationships between themselves and their subordinates
        - Preferring some over others
      - This is described as terrible leadership
    - Laisses-faire leadership allows the organization to run without real oversight
      - This type of leadership suffers from higher rates of carelessness
    - Ethical Leadership is thoughtful about safety, security, and the well-being of subordinates
      - Leads to a sense of belonging
      - Decreases the need for malicious behavior
- Subordinates/Employees
  - Most employees and subordinates are not a risk
    - They do their jobs and go about their business within acceptable variance
  - A subset of employees/subordinates will develop into “bad actors”
- Bad Actors
  - Five main types: Insider sabotage, exploitation, fraud, unintentional insider threat, workplace violence
    - Breaks down to Intentional versus unintentional threat
      - Similar to carelessness versus grievance
  - Narcissistic Employee
    - Will see themselves as a hero or doing the right thing
    - This is often really a sign of behavior and response to challenges to that identity
    - The intention is to do something that might be malicious, but in their mind, it might not be
  - Incidental Actor is the disgruntled or disengaged counterproductive employee
    - Vulnerable to accidental leakage
    - This can lead to careless behavior
    - They are more vulnerable to social engineering
  - Violent Actor
    - Threats, harassment, bullying, intimidation, physical violence
    - Could lead to targeted violence against an individual or the wider group
    - Vandalism, sabotage, and arson also fall in this category
  - MICE: Money, Ideology, Compromise, Ego
    - This is the classic acronym of insider threat

  - Money as incentive
  - Ideology as a competing belief system
  - Compromise as in blackmail or coercion
  - Ego as akin to narcissism, the need to feel bigger, better, or more important
- Critical Pathway Theory
  - Personal predisposition to be an insider risk
    - Involves medical and psychological disorders
      - Judgement, self-control, substance abuse
      - Serious psychiatric disorders
      - Personality disorders
        - Psychopaths, narcissists, “video voyeurs” (people who are paranoid, avoidant, and/or a bit removed from society), rule violators
  - Social Network Risks
    - Contact with outside groups
      - Extremist organizations, foreign government organizations
      - Family, friends, and marriage are the most common issues, followed by professional connections
      - Travel history is an important consideration
        - Repeated travel to locations with no connection to the location

Summary of the Public and Organizational Policy Panel

Bill Lucyshyn (Public Policy, University of Maryland)

The panel discussed the Federal supply chain security priorities and policies, operational challenges, and finally how policies are executed at the organizational level. The following points and questions were raised:

- The federal government has recently increased the emphasis on supply chain security as evidenced by Executive Order 14017 “America's Supply Chains”, the establishment of a federal supply chain task force, as well as numerous reports from federal departments and agencies, the Government Accountability Office, and Congressional Research Service.
    - Although these documents provide a lot of information, they are written at a high level and consequently challenging for businesses to translate into actions they can take.
    - The term “supply chain” does not adequately describe the environment, it implies linearity. However, in reality, what exists is a “supply web in ‘n’ dimensions”.
    - Most companies focus on short-term performance and end-of-quarter results. As a result, they are reluctant to make long-term investments that would reduce supply chain risk.
- In many industry sectors, companies can have very different supply chain structures yet have significant overlaps in their tier 1 and tier 2 suppliers.
    - For example, Dell and Lenovo share over 2200 suppliers. How much overlap is there in other industry sectors? How much do some of these supply chains also extend into other industry sectors?
    - In the defense sector, all of the major firms often rely on the same source (or two sources) for critical components but continue to tackle their common problems independently. There are no incentives to share information, there are in fact disincentives due to potential liability issues to share that information.
- Federal policy requires that those firms they do business with to manage their supply chain risk, however, this does not reduce the risk, but just transfers responsibility for monitoring and reducing it downstream.
    - However, the government still owns the risk.
    - There has been little willingness to say this is the government’s problem, that the government has to have a role besides including the appropriate clause in the contract. The reality is these clauses may or may not be complied with.
    - Risk is a trade space, and risk generally cannot be reduced to zero.
    - How much risk is the government willing to assume, and what needs to be done to mitigate it?
    - How do we prepare for risks that will occur that have not been mitigated?
    - How can these shared risks be managed in a way that enables us to do it effectively?
- Many vendors have exceptional products that can provide visibility into supply chains. How is that information being used now? How should that information be used to reduce or mitigate risk in a global marketplace?
- One approach with organizational policy is to get better data and incorporate the supply chain risk into the overarching approach for obsolescence i.e., in their approach for Diminishing Manufacturing Sources and Material Shortages (DMSMS).
    - This includes tracking where the Tier one suppliers are getting their components, but also includes where these suppliers get their parts, and even down to where the raw materials come from.

The following recommendations were suggested:

- The Federal Government must eliminate barriers and develop incentives for firms to increase information sharing related to supply chain risks.
- Most of our analysis, for the last number of decades, has been for point solutions. The entire range of possibilities is not adequately examined. Modeling and simulation should be used to examine these and develop better responses for a changing and very uncertain environment.
- The Federal Government should be more strategic in making investments in the manufacturing infrastructure
  - Government sponsors should consider providing extra funding to enable firms to develop additional sources for critical components.
  - One strategy that could support a second source is to use a dual-sourcing approach. For example, compete two sources annually, and then award contracts to both, using a 60/40 split to reward the superior performer.

Summary of the Modeling, Analytics and Data Panel

Peter Sandborn (Engineering, University of Maryland)

Three types of modeling are relevant to this space:

- System dynamics – macro level (top-down perspective). Maps a problem onto a generic structure that can aid in constructing an understanding of the underlying causes behind the behavior of the system. In system dynamics, the world is represented by a set of feedback mechanisms that produce dynamic changes in the system's behavior.
- Discrete-event simulation – meso level (workflow perspective). Replicates or emulates the structure of a process (e.g., the life-cycle of the system) and then allows performance to be measured under a number of scenarios. The world is a sequence of discrete events each of which changes the state of the system.
- Agent-based modeling – micro level (individual, bottom-up perspective). Models individuals or groups of "agents" whose actions are governed by their individual motivations. Overall system behavior inferred from the complex interactions between its agents.

One could model supply chains (networks) using any one of the approaches above, however, to capture the essence of supply-chain compromises, all three approaches need to be used in concert. The approaches above generally help predict the probability of an outcome, but they don't tell you what the optimal action to take based on that probabilistic outcome, for which you need:

- Decision model (action selection forecast) – based on a probabilistic outcome for a particular scenario, determine the best action(s) to take.

The workshop discussion included the following themes:

What is the motivation for modeling?

- Fundamentally, models increase efficiency (allow testing what-ifs against networks, allow optima to be found and scenarios to be tested) – building and observing real networks is impractical (is too cumbersome, too expensive, and takes too long).
- Models provide (or sometimes prove or disprove) intuition.
- Policy evaluation. We make policy based on what we have already observed. If something works keep it. If something doesn't work change it.
  - Some policies are straightforward, but others really need simulation.
  - Implementing bad policy is very expensive and may provide attack vectors for our adversaries.
  - Policies have unintended consequences.
  - Policy diffusion simulation
- Models can be used in the digital twins of supply chains, workforces, contracts, etc.

We must model humans in the loop

- Socio-technical modeling is needed (agent-based modeling is a way to do this).
- Machines authenticate, but humans trust.
  - Trust is the at the root of decisions
  - Desperate people make dangerous decisions

- The landscape is different for each agent, which is the intersection of a few "groups" a decision maker is part of. These groups restrict an agent's actions. Agents try to get to the lowest energy state (e.g., highest profit, lowest cost, largest value).
- How we interpret humans is different between modelers.
    - We should be using data to model how people behave.
    - It is important to model how agents learn.
    - Creating rule sets and action set for agents is difficult.
    - Modeling humans is better using psychologists, but subject expert matter should be better at letting go of parameters and simplifying. Modelers and psychologists meeting in the middle.

<u>Attack vectors</u>

- Disrupting things earlier in a network is better for our adversaries, therefore, network modeling is imperative.
- If you can mathematically find where the best place is for adversary to attack is (most bang for their buck). Defend that spot.

<u>What are the problems with modeling?</u>

- Simplifying models to the point where decision makers find them easy and useful.
    - Reduced order models are needed (models that require 10 inputs are much more useful than models that require 1000 inputs)
    - In most models requiring 1000 inputs, 990 of the inputs don't affect the answer.
- The model is also a communication device (not just an exploration or optimization device). The model can be interactive for decision makers to make it more appealing to them.
- Google and Amazon have amazing human data, how do we use that data to model human behavior with.
- Socio-economical modeling is also necessary.
- Have to meet decision makers (management, the customer) where they live, i.e., we need to generate metrics they understand in a way that they can grasp the impact (value) to the decision they are making.
    - Cost modeling is needed to make a business case for decision makers. Otherwise, no one listens.