2/24/2025

Team Meeting Notes:

Discussed how we missed a lot of points on technical plan, and the video didn’t include research questions.

Ask about getting super technical when he stated that our M2 might change a lot

Simulation: do we build a network of companies where a single point of failure happens, on one company and goes from 100% function to 50% function 🡪 how long do a set of “agents” lose.

2-3 attacks with different variables, set a population, set amount of production, EFFECT is the focus.

Variables: population, consumption, one agent consumes one pound per tick, supply chain is affected and how that effects companies and users.

Talk about maybe getting away from food production industry. Lots of benefits to sticking with that.

How do you want to apply NetLogo to research and project side of things 🡪 Ryan’s initial plan was to have JBS incident and their system down. The model would be on variables: type of attack, whether they paid the ransom, what security aspects were affected? (roles, IDS, etc.) What environmental aspects affected the attack?

Maybe we concentrate on two incidents and models where: a company like JBS that gets attacked and then CrowdStrike where the same software gets attacked (change control system) and the domino effect that has on additional companies/industries.

CASE STUDY ON CrowdStrike:

Extreme segregation is the only way defense against human error. Push update out to one directory at a time.

Local host versus cloud when deploying updates.

2/24/2025

Meeting with Dr. Hale

M1 Feedback – Timeline…. The high level meta needs to have in tasking workflow that “define what agents we will have in our model” and not just broad tasking. Lower-level things need to be broken down more to see what we need to prepare to submit the overall task

Getting specifics about incidents 🡪 what happened? How are we going to collect data in order to form our simulation models. **What is the level of granularity on the model?** What is the agent? Model the mean time to recover after infectivity

How likely is it for the infection to occur?

We are going to stick with Food Producer and CrowdStrike. Paper would focus on what happens when food supply goes down for 5 days, and CrowdStrike example.

Consolidated industries in general 🡪 couple examples that prove the overall same claim.

Use Stock Price as a proxy if no others can be found. Also, we could look at the number of units produced.

M1 Technical Plan – Steps 3 and 5 need way more detail. Is there data we can gather?

Step 3 – go back to the technical plan and input some of the things that we want to model. Given the specific examples/scenario 🡪 these are the aspects that we are going to extract from these. Build them into the model

Step 5 – Review then the modeling situation (out of order). One of the cases find out what happened, strip away the outcome and focus on the specifics before it happened. And simulate the model forward, does it behave the same way as it actually happened?

Also add one more step, validating what the model is actually doing.

Review of resources – find existing NetLogo models on GitHub or similar website and tweak existing models. It is not necessary to build models from the ground up.

Deliverable should be how we can gather a bunch of evidence and get a compelling argument for why consolidated industries should be more careful and how we could build evidence for why people/Congress should care. GET RATIONALE to POLICY MAKERS. (position paper) assumptions, why, a few examples, here’s some modeling environments, is a good way to advance the narrative.

What are the right parameters? Trial and error.

The why of what we are doing rolls into our position paper that is evidence for policy makers to use or cite.