Cyber Risks of Critical Infrastructure Consolidation and Homogeneous Software Adoption: Modern Nuance of Modern Warfare

Executive Summary

Modern infrastructure enables adversaries to disrupt organizations with cyber attacks. This problem is exacerbated when a single company dominates specific industries or services, such as banking, healthcare, or food production. This paper aims to develop policy recommendations to address cybersecurity risks associated with industry consolidation. For example, disruptions to food suppliers could lead to widespread food insecurity. If Big Poultry Corporation produces 75% of domestic poultry products, a cyber attack targeting them would create starvation conditions for large populations.

The risks to national security and societal stability are evident. It is crucial for the Federal Trade Commission to consider these cybersecurity threats when evaluating mergers and acquisitions (M&A) between large companies and for companies to incorporate these risks into their decision-making process.

Project Goals

- Create two agent-based models using NetLogo
    i. Network Attack
    ii. Effects of outage on Supply Chain
- Survey of IT and non-IT decision makers
- Analyze case studies of Crowd Strike and JBS cyber incidents

Project Realization

M3 Progress Report

Project Methodology

For our modeling we used a program called NetLogo. NetLogo is a programmable modeling environment used for simulating natural and social phenomena. NetLogo is agent-based, meaning it allows users to create and simulate the actions of individual "agents" (like animals, people, or vehicles) in a system to observe how complex behaviors emerge from simple rules.

NetLogo is free and supported by Northwestern University. It is an agent-based modeling tool that demonstrates how individual agents follow rules and interact with one another. It is available for Windows, Mac, and Linux and is as simple as requesting to download the installer, then running it. After that, an existing model can be imported and modifications made, or users can start from scratch. NetLogo models are written in a language called Scala.

Network Model

Network Model variables and parameters

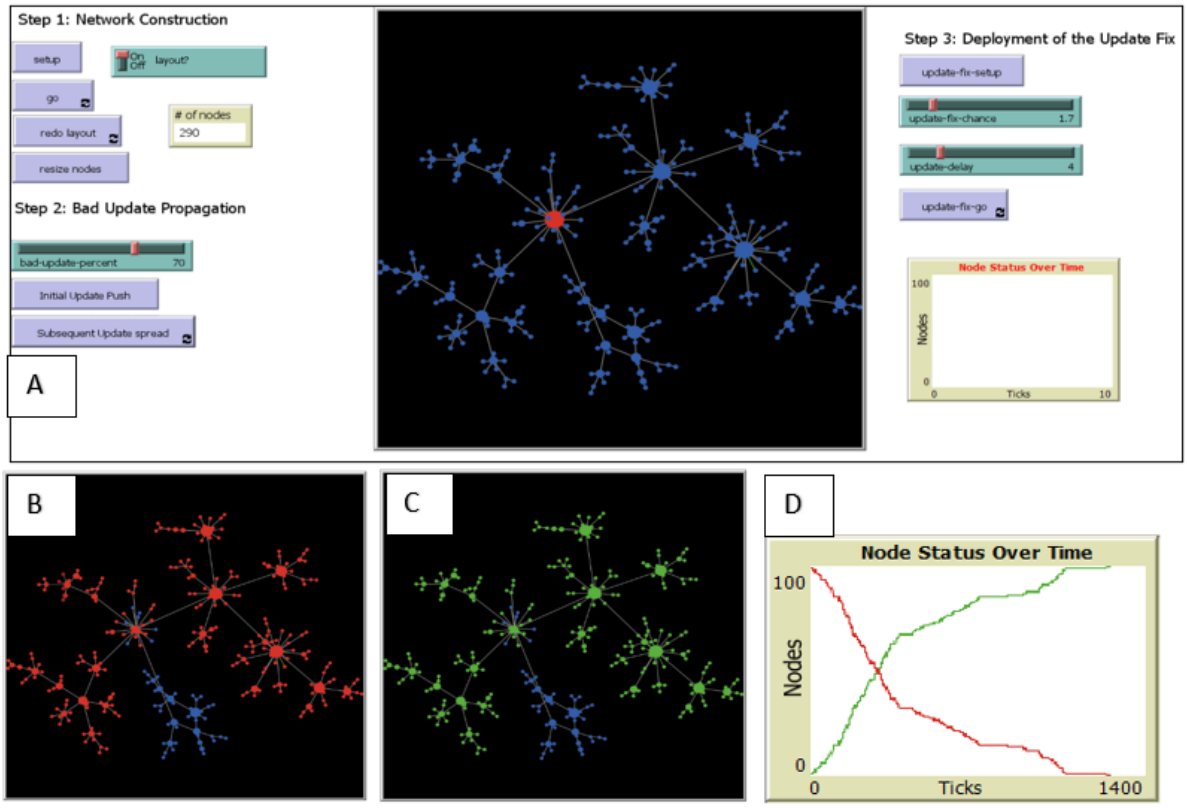


Figure 1 illustrates the stages of the network construction, propagation of the vulnerability, and deployment of a fix. **Figure 1A** is the dashboard for the AI model that depicts the fully constructed network, with the red node representing the initial point of interest or origin of the vulnerability. **Figure 1B** shows the propagation and spread of the vulnerability throughout the network, with compromised nodes highlighted in red. **Figure 1C** visualizes the deployment of the remediation or patch, where recovered nodes are marked in green. **Figure 1D** presents a graph illustrating the duration required for the update fix to successfully restore all affected nodes in the network. Throughout all stages, blue nodes represent unaffected nodes.

Step 1--- Network Construction

Setup: Button Resets the Network construction with 2 nodes. 1 blue node and 1 red node to represent where the vulnerability begins.

go: Button Initiates the creation of nodes that randomly connect to existing nodes in the

network. Pressing the button again will pause the node creation process. Generating between 200 and 400 nodes typically results in an ideal visualization of network structure and connectivity.
# of nodes: Counter Shows the number of nodes that are created.
redo layout: Button This button repositions the nodes to improve the visual clarity and organization of the network structure. Press the button again to pause the repositioning of the nodes.
resize nodes: Button Adjusts the size of each node based on its number of connections. The more connections the bigger the node will be.

Step 2--- Bad Update Propagation

bad-update-percent: slider This will be percent of connections that will receive the update/vulnerability that are connected to the initial red node.
Initial Update Push: Button This will push the update/vulnerability to the immediate nodes that are connected to the initial red node. The nodes are turned red and chosen at random based on the percent from the bad-update-percent slider. The initial red node that pushed the update/vulnerability will also change to a triangle to represent show where the inital vulnerability began.
Subsequent Update spread: Button This button will push the update/vulnerability to all subsequent nodes that are connected to the nodes that were chosen from the Initial Update Push, turning the nodes red. Push the Subsequent Update spread button to stop it before continuing the model. The blue node connections that did not receive the Initial Update Push will not be affected by the Subsequent Update spread and remain blue.

Step 3--- Deployment of the Update Fix

Note: Ensure that the Step 1 buttons (Go and Redo Layout) and the Step 2 button (Subsequent Update Spread) are stopped before proceeding. This ensures the graph accurately reflects only the actions taken during Step 3.
update-fix-setup: Button This initializes the network for the fix deployment phase by identifying and preparing the nodes that will begin spreading the update. It is represented by turning the initial node from red triangle to a green triangle.
Update-fix-chance: Slider This represents the rate a node will successfully transmit the fix to the connected nodes during each tick of the recovery phase turning the nodes green.
update-delay: Slider Specifies the number of ticks to delay the initiation of the fix deployment, representing the time required to identify the vulnerability and begin recovery efforts.
update-fix-go: Button Starts the propagation of the fix turning the nodes green across the network based on the configured delay and update chance. It simulates the recovery process from the vulnerability. The update will start at the Green Triangle Node and propagate only to the red nodes until all red nodes are turned green.

Node Status Over Time: Graph The graph displays the progression of node states throughout the simulation, tracking the number of vulnerable (red), and recovered (green) nodes over time in ticks.

Network Model Scenario

NetLogo version 6.4 was used to build the Network model and Supply Chain model. Version 6.4 can be downloaded at the NetLogo Download page.
The Network model can be found here at this link NetLogo Network Model.

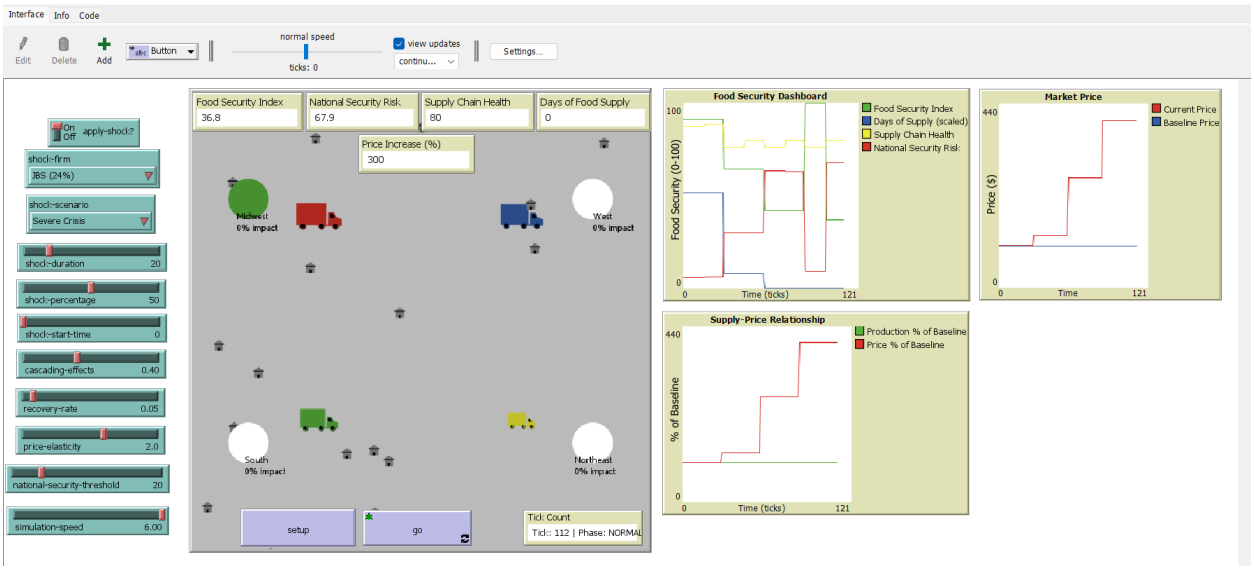
Crowd Strike Scenario--- This scenario is designed to simulate the network vulnerabilities associated with the CrowdStrike outage. It shows the effects of a potential cyberattack by illustrating how a network can be brought down, and the time it takes to bring the network back online.

- Step 2 bad-update-percent slider should be set at 70%. This shows that not all connections are part of the CrowdStrike program and that not all customers received the update.
- Step 3 set the update-fix-chance slider to 1.7 and the update-delay to 4.
- You can click the update-fix-go button to stop the model once all red nodes have turned green.

Conclusion of Scenario CrowdStrike

After the simulation, you will see the propagation of the bad update by the red nodes. Many nodes remain blue, indicating they never received the bad update and therefore do not require a fix. To simulate the real-world conditions experienced by CrowdStrike customers, the update-fix-chance was set to a lower value to reflect the recovery update that was pushed. The graph is measured in ticks, and each tick is equal to 30 min. All of the red nodes should turn into green nodes around 800 ticks. This is about 2 weeks and represents the time to fix 99% of all computers/servers that received the real-world update fix from CrowdStrike.

Supply Chain Model



The Supply Chain model can be found here NetLogo Supply Chain Model
The Supply Chain Control Manual can be found Here
The Supply Chain Setup Guide can be found Here

Below is a detailed explanation of each parameter in the Supply Chain Model:

Initial Conditions: Each firm starts at full production capacity, 14 days of meat supply in the system, and has a food security index of 100 (best case).
Shock Scenarios: Mild – A small-scale attack with 10% production loss and a 5-tick recovery.
Recovery – A moderate attack with 30% production loss, 20-tick recovery, but has industry support for recovery.
Severe – A major cyber attack with 50% production loss and a 30-tick recovery time.
Key Parameters: Shock duration: Number of ticks that the initial "shock" lasts. (0-30)The greater the duration, the greater the disruption (0-30)
Shock percentage: Production reduction during shock (10-70%). It represents the total immediate production reduction.
Recovery rate: Speed at which the affected firms recover (1-50%) per tick.
Cascading effects: The rate at which disruptions spread to other firms (0 – 100%) The higher values mean the supply chain is affected more.
Price elasticity: How prices respond to changes in supply. (.5-3.0) The higher values create more dramatic price hikes.
Shock-start time: This is the tick number when disruption begins. It allows for observing baseline values before a shock happens.
National security threshold: The risk level that simulates national security concerns (0-100). The higher the value, the more sensitive the model will report national security risks.

The lower threshold means that the model will only report national security risks only in severe situations.

Survey of Professionals

- Problem was presented to local DEFCON meeting of ~40 local professionals
- Survey sent to other business social groups
- In total the survey was sent to ~100 individuals
- 26 responded and 1 respondent was tossed out, leaving 25 total responses
- The following three were deemed most relevent to our final report:
    - When asked whether market share influences software adoption, 50% of respondents answered yes, while 50% answered no.
    - When evaluating widespread adoption, 16% viewed it as extremely positive, 40% somewhat positive, and 44% neutral. None saw it as negative.
    - Regarding perceived risk, 4% saw a high risk, 43% medium, 44% low, and 8% near zero.

Analysis of Case Studies

- A case study of the JBS attack in May of 2021 was used as evidence to support claims made in the executive summary
- A case study of the CrowdStrike incident of 2024 was used as evidence to support claims made in the executive summary

Results / Findings

The most detailed report of our outcomes for each milestone can be found Here

M1

- Original scope was too large i.e. trying to affect current policy is not achievable within the given time range
- Scope was adjusted to create evidence using modeling, surveys and analysis of existing case studies
- This evidence would be used to support our thesis and, as far as we can tell, be one of the first papers on the subject as it relates to modern cyber risks

Findings of Lit Review

- Research on this specific subject is nearly non-existent
- Some references to risks of consolidation within the defense industry were addressed by military organizations, including preventing mergers that would create too large of a single point of failure in say, ammunition production

M2

Results of Survey (25 respondents)

- When asked whether market share influences software adoption, 50% of respondents answered yes, while 50% answered no.
- When evaluating widespread adoption, 16% viewed it as extremely positive, 40% somewhat positive, and 44% neutral. None saw it as negative.
- Regarding perceived risk, 4% saw a high risk, 43% medium, 44% low, and 8% near zero.
- Most respondents did not associate widespread adoption with higher risk, reinforcing the belief that market dominance suggests reliability, soundness, or superiority in the most generic sense.

Findings of Case Studies

JBS Attack

- REvil monetized access to victim networks and sold that access to other REvil affiliates.
- Before encrypting victim organization networks, REvil used double extortion methods to first steal sensitive data from victims and then publish that data on REvil's public blog.
- REvil harassed victim company employees via email and telephone to coerce the companies into paying ransoms
- USDA instructed competitors to increase output
- JBS was dark for a full day and incrementally came back over three days

CrowdStrike Incident

- Systems administrator at CrowdStrike caused the largest IT outage in American history
- System administrator performed a windows update which was neither validated, verified, nor followed the change management approval process
- There was a security flaw discovered in the Falcon sensor version 7.11 and above which caused the system to crash
- Billions of dollars in lost productivity and chaos

Summary of Findings/Implications

For Milestone II, a key accomplishment for the team included developing a survey to use to build out metrics for the NetLogo model. Conducting the survey helped the team understand which variables we could use for our NetLogo data model. We also encountered several issues and challenges associated with our project. For example, some of the issues we encountered included availability of personnel, loss of power and understanding the data to generate different scenarios for data modeling. The team was able to overcome these obstacles by conducting meetings to discuss ongoing issues and assigned tasks for the milestone II deliverable.

M3

Findings of Network Model

The network model demonstrates how quickly a mistake can propagate through networks. Researchers based this model on a real-world incident, revealing the negative impact and implications. Future attacks will likely draw inspiration from this incident, despite the outage resulting from cyber negligence rather than a cyberattack.

Findings of Supply Chain Model

The supply chain model effectively demonstrates the downstream result of an extended outage in the food processing industry. Longer outage shows a significant drop in production. Depending on severity, if this outage occurs with the largest supplier, competing firms cannot make up for the lost production. The model did not include a calculation of how long the food supply could support the population before leading to famine i.e. agent death. This functionality would be the next logical step in its development.

Summary of Findings/Implications

For Milestone III, our team focused on completing the necessary steps in the last phase of the project. These steps will include deliverables such as testing and validation, user instruction documentation and technical documentation. All other key deliverables, such as the graduate research paper and other documentation will be included in the overall package as the final project deliverables. During the last several weeks, our team encountered several issues and challenges in completing the final phase of the project. These issues and challenges include availability of personnel, inclement weather to include loss of power, learning curves related to the project and finalizing the research paper. The team was able to overcome these obstacles by conducting meetings to discuss ongoing issues and resolutions to assigned tasks for the milestone III deliverable.

Most organizations see large market share as a positive sign when choosing software, equating it with product reliability and success. However, this widespread adoption creates interconnected systems that are increasingly vulnerable to cyber disruptions. While past disruptions required massive resources, today's attackers can achieve similar damage with minimal effort. The survey reveals a general lack of awareness about these risks. One proposed solution is breaking up overly large corporations using existing antitrust laws, while another is implementing extreme segregation within organizations as they grow or prepare for IPOs to enhance cybersecurity**.**

Install and Release

Due to objections from team member(s), no release version or information will be provided.