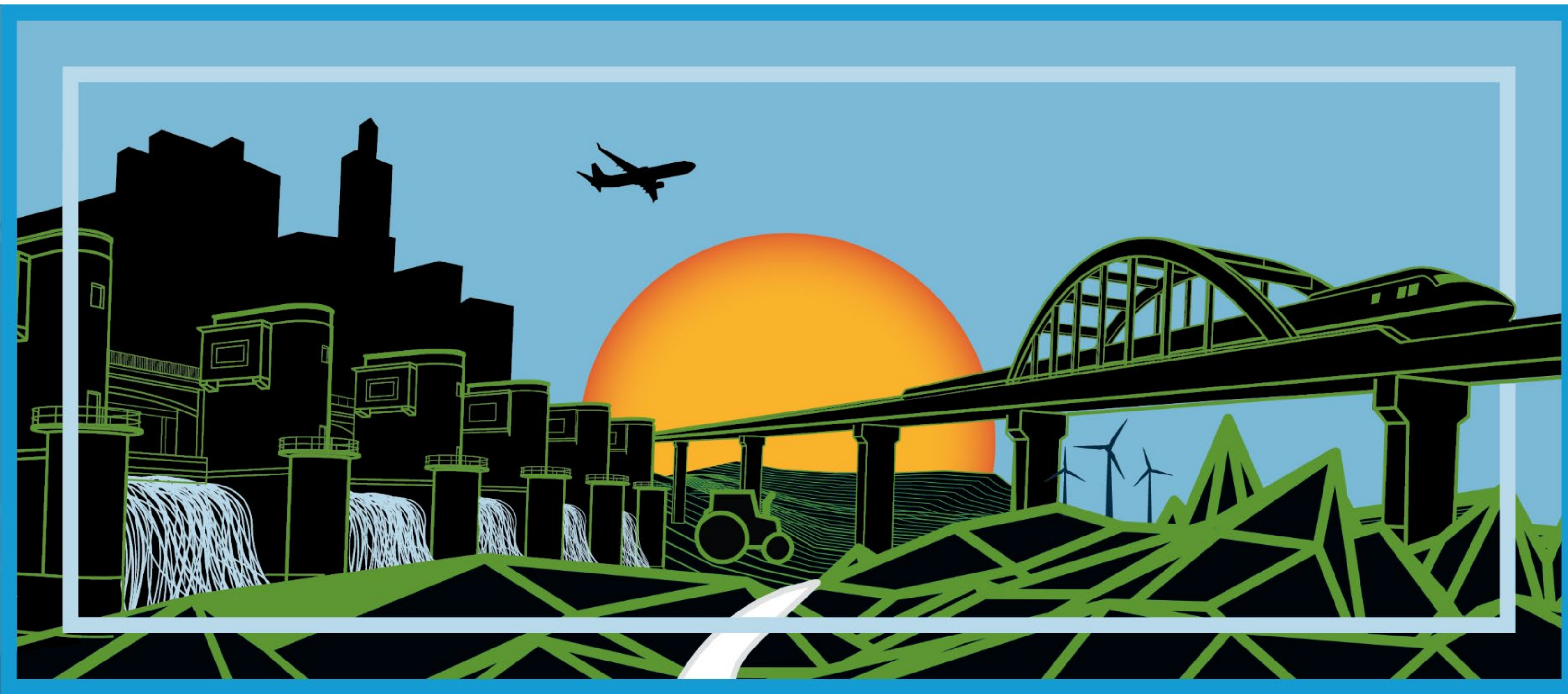

Secure Tomorrow Series

Alternate Futures: ICT Supply Chain Resilience Player Guide

Publication: June 2024
Cybersecurity and Infrastructure Security Agency

BACKGROUND

How prepared are critical infrastructure sectors in light of potential challenges to the resilience of the information and communications technology (ICT) supply chain? *Alternative Futures: ICT Supply Chain Resilience* presents you with scenarios that could plausibly occur within the next three to seven years. During each round, you and your opponents will take turns proposing initiatives and debating strategies that will shape critical infrastructure resilience and security in light of potential challenges to the security and stability of the ICT supply chain. How successfully you manage to present your arguments for (or against) these initiatives determines their chances of success. Depending on your role for the round, you can score points for either successfully implementing or countering initiatives.

The Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center has developed this game to assist stakeholders across the critical infrastructure community to self-facilitate and conduct foresight activities that will enable them to derive actionable insights about the future, identify emerging risks, and proactively develop corresponding risk management strategies to implement now. One goal of the Secure Tomorrow Series is to develop a repeatable and defensible process that (1) identifies emerging and evolving risks to critical infrastructure systems, and (2) identifies and analyzes the key indicators, trends, accelerators, and derailers associated with those risks to help critical infrastructure stakeholders direct their risk management activities.

For players, the game hopefully represents a fun and interactive way for you to think broadly about future threats and opportunities, learn from your peers, and identify strategies to inform preparedness activities.

The game takes about three hours to complete. This includes an introduction and description of the current state, three rounds of gameplay (each about 45 minutes long), and a final 20-minute open-discussion period to collect any final feedback from players and wrap up the game.

PLAYER ROLES AND ASSIGNMENTS

At the start of the game, each player will be assigned one of three roles. Players will rotate roles in subsequent rounds, so that they fill different roles through the course of the game. The three roles are as follows:

- The Innovator(s): Responsible for developing initiatives and arguments in support of those initiatives.
- The Devil's Advocate: Responsible for developing counterarguments to the initiatives proposed by the Innovator.
- The Judge: Responsible for adjudicating the validity of the Innovator's arguments versus the counterarguments made by the Devil's Advocate for a particular initiative and determining the initiative's likelihood of success.

Players will bring their personal knowledge, experience, and perspectives to debate strategies that will shape critical infrastructure resilience and security in light of potential challenges to the ICT supply chain. Players should consider policies, programs, investments, public-private partnerships, research and development, or other actions that, if successfully put into motion today, they believe will better position and prepare one or more critical infrastructure sectors for the future. In preparing for the game, players may want to think about the following questions:

- What risks and opportunities are associated with current trends in ICT supply chain resilience?
- What are the implications for future critical infrastructure resilience and security?
- Are there specific ramifications for one or more critical infrastructure sectors?
- Is there a role for CISA to address threats and uncertainties associated with ICT supply chain resilience?
- Are there other trends that may influence ICT supply chain resilience in the future?

PRESENT STATE

The ICT supply chain consists of the hardware components, protocols, and software that make up the modern internet and telecommunications technology. The ICT supply chain is integral to the daily operations and functionality of U.S. critical infrastructure. This ecosystem contains a wide variety of interconnected systems and actors including third-party vendors, suppliers, service suppliers, and contractors, all of whom are vulnerable to being targeted and potentially compromised by malicious actors. Currently, the United States remains a global leader across much of the ICT supply chain, particularly in innovation and development; however, other countries lead in the production of many components.

ICT supply chain risks often involve the exploitation of vulnerabilities that exist throughout the ICT lifecycle. These risks include malicious software and hardware; counterfeit components; poor product designs; manufacturing processes; and maintenance procedures. When supply chains are compromised successfully, adversaries may conduct espionage, sabotage, data and intellectual property theft, and cause outright system failure. The ramifications of such intrusions may pose existential risks to individual businesses.

Current trends influencing future developments in ICT supply chain resilience include the following:

- Malicious actors may use artificial intelligence to facilitate cyberattacks.
- Foreign manufacturers may achieve market dominance in 5G components.
- Because of geopolitical pressures, global supply chains may shift to domestically controllable supply chains to enhance national security.
- The use of edge computing and software-defined networks will increase.
- The United States will compete for influence in international internet standard-setting bodies.
- As device and computational demands grow, the United States will be challenged to provide reliable energy.

Many of the trends will necessitate effectively applying supply chain risk management; developing policies and procedures; understanding the hardware and software; the services that are procured; knowing the suppliers involved; determining how to assess the security of suppliers; and establishing timeframes and systems for checking supply chain practices against guidelines.

PLAYING THE GAME

Alternative Futures: ICT Supply Chain Resilience has three rounds, each of which will present the players with a scenario that could plausibly occur within the next three to seven years. In Round 1, the Innovator(s) will have 15 minutes to identify up to three initiatives that will support critical infrastructure resilience and security in response to the specified scenario disruptor. For each initiative, the Innovator(s) will then describe up to three supporting arguments for why the initiative will succeed. The Devil's Advocate will then have 10 minutes to describe up to three counterarguments for each initiative. Each counterargument can be directed at one or more of the arguments presented in favor of the initiative's success or underscore a new concern that may cause the initiative to fail. The Innovator(s) will then have five minutes to rebut any or all of the counterarguments. The Judge will listen to both sides of the debate and ultimately determine if each initiative has a high, medium, or low likelihood of success. The Judge will have 5 minutes to present the rationale for his or her determinations and roll a 20-sided die to see if each initiative succeeds or fails.

The die simulates the unpredictability of the supporting environment for initiatives, and the game's inability to account for all positive and negative factors that might influence success.

- An initiative with a **high** likelihood of success will be implemented with a roll of 6 or higher (75 percent chance).
- An initiative with a **medium** likelihood of success will be implemented with a roll of 11 or higher (50 percent chance).
- An initiative with a **low** likelihood of success will be implemented with a roll of 16 or higher (25 percent chance).

An open-discussion period may occur after resolving the success or failure of the initiatives to continue any discussions cut short by previous time constraints.

In Rounds Two and Three, the participants will rotate roles.

DISRUPTORS

Social, technological, environmental, economic, and political (STEEP) influences have the potential to alter the trajectory of future trends or disrupt them altogether. For example, urbanization is a social disruptor that has the potential to significantly affect the resilience of lifeline sectors and cyberattacks are a technological disruptor with a wide range of cascading implications for all critical infrastructure sectors.

To account for a changing future environment, each round features a STEEP disruptor scenario that may limit player actions, reflect changes in ICT supply chain resilience, or require players to consider the implications of an event. The possible scenarios to choose from during the game are described in Appendices I–V. As an added incentive for players to craft compelling arguments and counterarguments, the winning player of each round is awarded the ability to select the STEEP disruptor category for the next round.

WINNING THE GAME

If the Innovator(s) successfully implement(s) a majority of the initiatives, the Innovator(s) win(s) the round. Alternatively, if the Devil's Advocate counters a majority of the initiatives, he or she wins the round. While the game is designed to encourage competition between the players, its main purpose is to generate discussions that develop well-conceived and thought-provoking initiatives. Your collective subject matter expertise is what matters, regardless of the outcomes of each round.

GAME SCHEDULE

Table 1: Schedule for Conducting the Matrix Game

MATRIX GAME STAGES (~3 HOURS)				
Introduction	-	Welcome participants and discuss game purpose (Controller)	3 Min	18 Min Total
	-	Explain game rules (Controller)	5 Min	
	-	Practice round	7 Min	
	-	Introduce current state and potential implications (Controller)	3 Min	
Round 1	-	Introduce future scenario based on STEEP disruption (Controller)	5 Min	41–51 Min Total
	-	Craft initiatives and present arguments (Innovator(s))	15 Min	
	-	Present counterarguments (Devil's Advocate)	10 Min	
	-	Rebuttal (Innovator(s))	5 Min	
	-	Adjudicate arguments and roll die (Judge)	5 Min	
	-	(Optional) Open-discussion period	< 10 Min	
	-	Select STEEP disruptor	1 Min	
Round 2	-	Introduce future scenario based on STEEP disruption (Controller)	5 Min	41–51 Min Total
	-	Craft initiatives and present arguments (Innovator(s))	15 Min	
	-	Present counterarguments (Devil's Advocate)	10 Min	
	-	Rebuttal (Innovator(s))	5 Min	
	-	Adjudicate arguments and roll die (Judge)	5 Min	
	-	(Optional) Open-discussion period	< 10 Min	
	-	Select STEEP disruptor	1 Min	
Round 3	-	Introduce future scenario based on STEEP disruption (Controller)	5 Min	40–50 Min Total
	-	Craft initiatives and present arguments (Innovator(s))	15 Min	
	-	Present counterarguments (Devil's Advocate)	10 Min	
	-	Rebuttal (Innovator(s))	5 Min	
	-	Adjudicate arguments and roll die (Judge)	5 Min	
	-	(Optional) Open-discussion period	< 10 Min	
Wrap Up	-	Determine final game status of critical infrastructure security and resilience (Controller)	5 Min	20 Min Total
	-	Open-discussion period (Players)	15 Min	

The Cybersecurity and Infrastructure Security Agency (CISA) has produced these scenarios to initiate and facilitate discussion. The situations described here are hypothetical and speculative and should not be considered the position of the U.S. government. All names, characters, organizations, and incidents portrayed in these scenarios are fictitious. Any positions expressed by fictional characters herein regarding any particular issues or technologies do not represent the positions of CISA or the federal government.

APPENDIX I: SOCIAL DISRUPTOR

PERSONALITY PROFILES STOLEN

By 2030, most Americans regularly use the platform XYZ in their daily lives for immersive experiences. To connect its users optimally with experiences on the platform, XYZ collects an enormous amount of data about its members, which the platform leverages to build individual personality profiles.

In 2030, a criminal hacker breaches the XYZ databases and leaks all of the company's personality profiles on the dark web. Although the leaks do not include passwords or biometric data, they do include in-depth details about individuals' tastes and preferences. Malicious actors use the personality profiles to conduct spear phishing attacks, increasing their success rates considerably. A wave of cybercrime ensues, leading to significant increases in ransomware, stolen credentials, and other forms of social engineering–based intrusion and theft.

What initiatives are necessary to protect the user data being used to support increasingly sophisticated analytic capabilities?

APPENDIX II: TECHNOLOGICAL DISRUPTOR

COUNTERFEIT COMPUTER COMPONENTS

In 2026, an information technology (IT) manager at a facility finds that a server has overheated and shutdown. After swapping out the damaged components and bringing the system back online, the IT manager investigates the problem. According to the logs, the room temperature was stable and no other nearby servers overheated. She assumes that the damage was the result of an isolated incident, most likely a faulty component, and reports the incident to the IT procurement team.

Upon further investigation, the procurement team discovers that the server in question had been updated with a new set of CPUs shipped from a supplier 10 months prior to the incident. These CPUs had been distributed throughout supply chains for use in a wide variety of systems. The supplier has provided components to the facility for years without any issues. Furthermore, other recent cases of overheated components have not been reported.

Out of an abundance of caution, the procurement team tasks a cyber protection team (CPT) to scan a few of the servers that are running with the new CPUs. After noticing immediately that some components are drawing more computer power than is necessary, the CPT discovers a program on one of the servers that is copying and covertly exfiltrating data. The CPT's final report expresses high confidence that the components are counterfeit and compromised for the purpose of espionage. Later on, investigators discover that the components were built using modern techniques to precisely replicate the CPUs used normally. As a result, the procurement team's standard counterfeit-detection process failed to identify these components and numerous networks may have been compromised.

What initiatives could help mitigate the risk of counterfeit or compromised computer components being used to infiltrate sensitive systems?

APPENDIX III: ECONOMIC DISRUPTOR

GLOBAL LITHIUM SUPPLY LAGS BEHIND DEMAND

Lithium-ion batteries for smartphones and other portable electronic devices are a key component of the ICT supply chain, and by 2030 the information technology sector faces intense competition for lithium batteries from other sectors including transportation, manufacturing, and energy.

As a result, market demand for lithium has increased dramatically. Supplies of lithium; however, have lagged behind demand. The supply chain for lithium is not yet a reliable global market and only a handful of countries have deposits that are economically viable for extraction. The supply shortage of lithium is leading to price increases and production delays across the ICT supply chain.

An even greater concern is refining capacity. By 2030, one foreign country controls half of the world's lithium processing capacity, leading to concerns about what would occur if it was to decide to restrict exports of processed lithium. Since battery technology is a dual use technology with a variety of military applications, there is concern about reliable access to lithium in the future.

What initiatives can you think of to address the limited supply of lithium and resulting high costs for battery manufacturing?

APPENDIX IV: ENVIRONMENTAL DISRUPTOR

CHIP MANUFACTURING IN DROUGHT CONDITIONS

In 2024, the semiconductor company Zuper Chipx completes construction of two chip fabrication plants that use ultra-purified water for cleaning the silicon wafers serving as the backbone of its chips. The two plants source the water from onsite groundwater wells.

By 2030, the state where these plants are located has experienced several years of drought and intense heat, during which businesses have been using groundwater much more quickly than it can be replenished naturally. As a result, Zuper Chipx is competing with numerous other industries statewide for rapidly shrinking groundwater resources. There are very limited alternative water sources, and the governor has mandated water-usage restrictions under a state of emergency.

Under these restrictions, the two fabrication plants can operate at only 75 percent capacity and must shutdown early every day to conserve water. Without urgent action, the plants may not have enough water to operate profitably and could be forced to close, an outcome that would have profound effects on U.S. national security and the ICT supply chain at large.

What initiatives can you think of to safeguard domestic production of semiconductor chips and other materials within the ICT supply chain against the future possibility of decreasing water availability?

APPENDIX V: POLITICAL DISRUPTOR

INTERNET PROTOCOLS STAGNATE

The international standard-setting body XYZ is responsible for developing the technical standards of the internet protocol suite. Since its formation, IOP has operated on a "rough consensus"-driven governance model, with the goal of an open global internet. Throughout much of its history, XYZ has worked hard to build improved security and end-to-end encryption into internet protocols.

However, by 2030, leadership of XYZ is roughly evenly split between two coalitions. One advocates strongly for improvements in internet privacy and security, while the other sees the internet as a tool for supporting commerce.

These colliding views of internet governance have left XYZ frozen, unable to craft new policy without the rough consensus of its members. As a result, progress on internet protocol security and privacy has stagnated. XYZ's governance structure was not designed to operate under these conditions, and the status quo risks undoing decades of progress on global internet governance.

What initiatives can critical infrastructure operators adopt in the interest of ensuring secure continuity of operations, despite the global governance challenges outlined in this scenario?