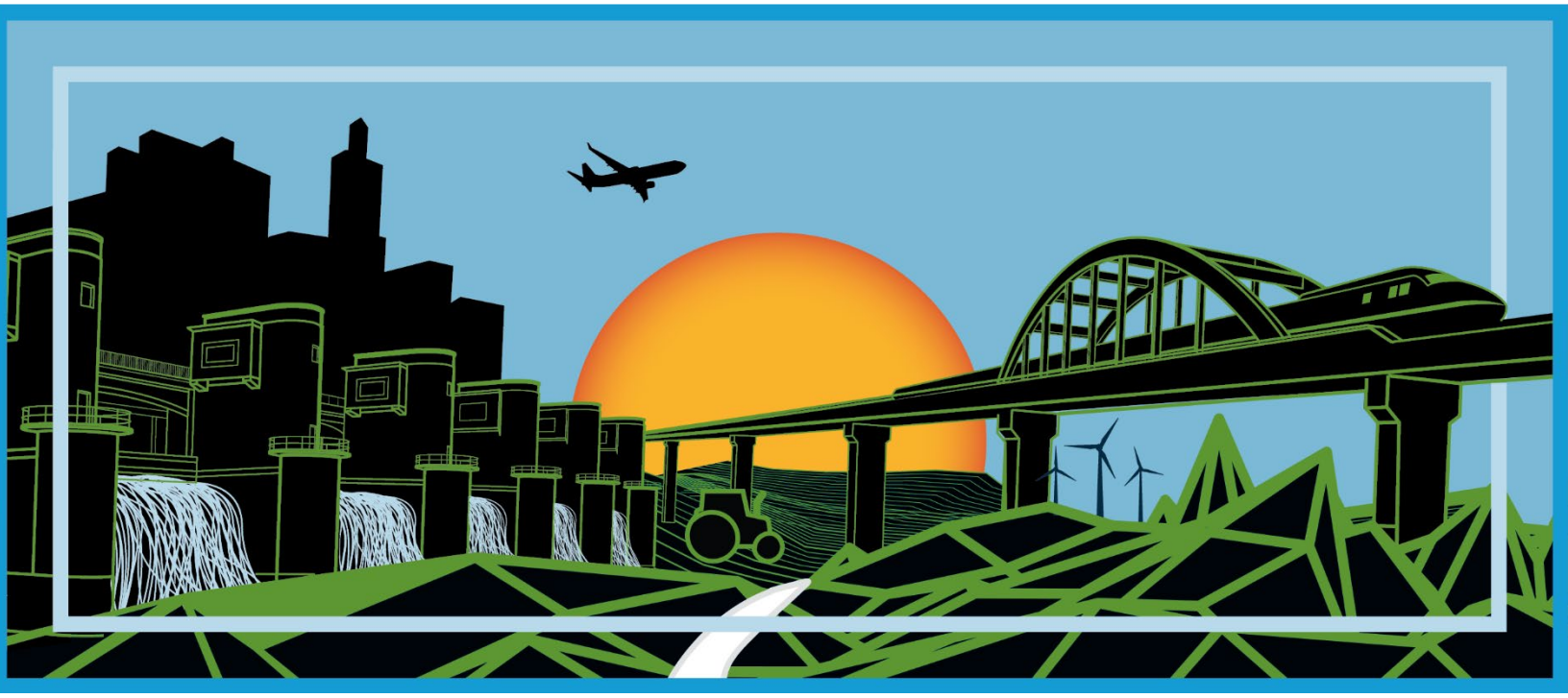

Secure Tomorrow Series

Alternate Futures: ICT Supply Chain Resilience Controller Guide

Publication: June 2024
Cybersecurity and Infrastructure Security Agency

WELCOME AND INTRODUCTIONS

[The instructions in this guide are built around a virtual execution of the workshop, using a virtual meeting platform.]

Hello. My name is [name], and for the next three hours I will be your game controller for Alternative Futures: ICT Supply Chain Resilience. My role is to guide you through the game.

Before we get started, let's do a quick round of introductions. [Ask players for their name and a quick summary of their background.]

The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center (NRMC) 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.

As such, today you will be playing as yourselves, bringing your knowledge, experience, and perspectives to debate strategies that will shape critical infrastructure resilience and security in light of potential challenges to the security and stability of the information and communications technology (ICT) supply chain. Hopefully, the game will be 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 consists of three rounds, each of which will present you with a scenario that could plausibly occur within the next three to seven years. During each round, you will play one of three unique roles. [Display placemat document on camera and point to the appropriate column header for each role as you name them.] *The three roles are the Innovator, the Devil's Advocate, and the Judge.* [Assign which player has what role for Round One. If there are more than three players participating, assign them to be additional Innovators.] *We will rotate roles after each round.*

What do these roles entail?

- ***The Innovator(s)**: Your job is to propose initiatives that will help critical infrastructure owners increase the security and resilience of their systems in preparation of future challenges to the resilience of the ICT supply chain. Initiatives could be policies, programs, investments, public-private partnerships, research and development, or other actions that, if successfully put into motion today, you believe will better position and prepare one or more critical infrastructure sectors for the future. You will have 15 minutes to think of and present up to three initiatives and up to three supporting arguments per initiative. When proposing an initiative, please consider both its potential effects and the feasibility of implementation.* [Note: If there is more than one Innovator per round, each Innovator will introduce at least one of the three initiatives. All Innovators will develop these initiatives collaboratively, attempting to bolster the supporting arguments. Please be flexible on the 15-minute time limit, especially in cases in which there are multiple Innovators and during the first round.]
- ***The Devil's Advocate**: Your job is to "stress test" the ideas of the Innovator(s). After the Innovator(s) finish(es) presenting the initiatives and supporting arguments, you will identify counterarguments as to why these initiatives may not be successful. In total, you will have*

10 minutes to present up to three counterarguments for each of the proposed initiatives. Your counterarguments can target one or more of the supporting arguments or can underscore a new concern that may cause the initiative to fail. You can choose to debate the effects the ideas will have or highlight challenges with implementation. Please note that the Innovator who proposed the initiative gets one last chance to rebut your counterarguments once you are finished.

As you've probably guessed by now, these two roles are competing against each other through your arguments and counterarguments. Depending on your role, you can score points for either successfully implementing your initiatives or denying your opponent's initiatives. Meanwhile, each successful initiative increases resilience to possible social, technological, economic, environmental, or political (STEEP) disruptions. [Display the STEEP Disruptors & Odds Poster on camera.]

- ***The Judge:*** *Your job is to weigh the arguments versus counterarguments for each initiative and determine whether it has a high, medium, or low chance of success.* [Display placemat document on camera and point to a row in the Judge's column that lists "Chance of Success."] *To be clear, "success" means the initiative can be implemented and, if implemented, will substantially increase security or resilience against possible threats arising from the described scenario. As the Judge, you may interject at any time for clarification, but please be careful not to influence or aid the other players' arguments or counterarguments.*

The Judge will determine the success of each initiative by rolling this virtual 20-sided die: https://rolladie.net/roll-a-d20-die. 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. [Display the STEEP Disruptors & Odds Poster on camera.]

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

Are there any questions so far?

*As a final note about these roles, please understand that this game **does** encourage you to compete with one another, but the **purpose** of this game is to generate discussions that develop well-conceived and thought-provoking initiatives. Regardless of the outcomes of each round, it is your collective insights that matter.*

Please use the placemat document you received to take notes and sketch out your arguments or counterarguments for each initiative.

PRACTICE ROUND

To familiarize yourself with the three roles, let's walk through a practice round with one initiative using a completely unrelated topic. As the topic, let's use "reducing the number of car accidents in the United States."

[Motion to Player One.] *What is one initiative that you think might help reduce the number of car accidents occurring nationwide each year? Now, provide a supporting argument why you think that*

this initiative would be successful, considering both how the initiative would affect the number of car accidents and how it could be implemented feasibly.

Normally, you would provide two more supporting arguments for this initiative, as supported by your fellow Innovators. You would then repeat this for up to two more initiatives. For this practice round, I'm going to move on to the Devil's Advocate.

[Motion to Player Two.] *As the Devil's Advocate, what is one reason why Player One's initiative might fail?*

Normally, you would identify up to three counterarguments for each initiative. After you come up with your counterarguments, we would go back to the Innovator(s) for a rebuttal.

[Motion to Player One.] *Do you have a quick rebuttal?*

[Motion to Player Three.] *Now, Judge, do you think this initiative has a high, medium, or low likelihood of success? Why? Finally, let's roll the die to see whether the initiative is ultimately a success or failure.*

[Determine whether successful.]

Now that we've done a practice round, are there any final questions? Does everyone understand the flow of the game? How about the odds? [Answer any questions.]

If there are no more questions, let's move on to the actual game.

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 most often involve the exploitation of vulnerabilities that exist throughout the ICT lifecycle. These risks include malicious software and hardware; counterfeit components; and 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 aforementioned trends will necessitate effectively applying supply chain risk management; developing policies and procedures; understanding the hardware, software, and 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.

Select a STEEP Disruptor

[Point to the STEEP Disruptors & Odds Poster.] *As I mentioned before, this poster outlines a popular framework for scanning the future. It covers five dimensions—social, technological, economic, environmental, and political—which make the acronym* STEEP.

Each disruptor will force players to explore strategies to mitigate risks to critical infrastructure during a plausible future scenario that could arise pertaining to the ICT supply chain. These scenarios may limit player actions, reflect changes in ICT supply chain resilience, or require players to consider the implications of an event. [Identify the first player to log on by name.] *As the first player to log on, you can choose which STEEP category you would like to explore for Round 1.* [See Appendices I–V. Please note that each disruptor ends with a question that should be announced to the group after reading through the disruptor narrative, to clarify the issue that players will be addressing for the disruptor. Additional discussion questions are included in each appendix to serve as prompts or as questions for open discussion periods.]

LET'S PLAY

Round One

As a reminder, for Round One you are considering initiatives that, if successfully begun today, you believe will help prepare critical infrastructure owners for potential risks arising in these future scenarios.

[Turn to the Innovator(s).] *I am going to begin your turn by giving you five minutes to gather your thoughts about potential initiatives. After that point, I will encourage you to share your thoughts aloud so that the other players can get a sense of what you're thinking. I'll be engaging you in a dialogue to help you flesh out your initiatives and develop the supporting arguments.* [If there are multiple Innovators, you may want to encourage the Innovator team members to begin sharing their ideas with each other after two minutes, before asking them to announce their first initiative after 5 minutes has elapsed.]

As a recommendation, try to stay away from sweeping generalizations. With such statements, I will push you to provide an example of what you are alluding to or ask you to give an anecdote to explain or demonstrate your idea. Innovator(s), your turn starts now.

[Start the timer from 15 minutes. After five minutes, prompt an Innovator to begin verbalizing their first initiative.]

Try to have the Innovator(s) frame arguments by explaining:

- How their idea addresses security and resiliency
- How the idea can be implemented

- What will change if the idea is implemented

Some questions to help the Innovator(s) develop supporting arguments include the following:

- Is there a precedent for the type of activity you are proposing?
- Are there major risks that need to be addressed in your supporting arguments?
- Are multiple steps necessary for implementation? What do you think might realistically be achieved in the next three to seven years?
- Who are the stakeholders necessary for implementation to be successful (i.e., whose support do you need)?
- What conditions exist today that make you believe this initiative will succeed (as opposed to in the past)?

Throughout the Innovator(s) round, or after 15 minutes, recap the Innovator(s) initiatives and supporting arguments and look to each Innovator to validate.

[Reset the timer to 10 minutes.] Ask the Devil's Advocate to begin thinking aloud and presenting their counterarguments. Start the timer.

Throughout the Devil's Advocate's round or after 10 minutes, recap the points made by the Devil's Advocate and look to the Devil's Advocate to validate.

[Reset the timer to five minutes.] Ask the Innovator(s) to begin their rebuttal and start the timer.

After the rebuttal period, ask the Judge to select the likelihood of success for each initiative and to present their rationale. Afterwards, direct the Judge to roll the die once for each initiative.

Declare the winner for Round One. [If there was a good discussion among participants during the round, you may want to include a short open discussion period (less than 10 minutes) following judgment to continue this discussion. This is also an opportunity to discuss how the initiatives could be strengthened.]

[Gesture to the Round One winner.] *As the winner of Round One, you get to choose the STEEP disruptor category for Round Two.*

Subsequent rounds

Assign new roles.

Present the new scenario based on the STEEP disruptor chosen (see Appendices I–V). [Please keep in mind that depending on what players present in the prior round, you may want to preclude them from selecting certain STEEP categories, since the discussion may become repetitive. Use your best judgment.]

Follow the instructions listed under Round One.

Declare the winner for Rounds Two and Three based on the results.

Direct the winning player or team to select a STEEP disruptor (Round two only).

[You can adjust the number of disruptors explored as desired, but you will need to consider the corresponding increase or decrease in time commitment and modify the gameboard, as necessary.]

WRAPPING UP AND FINAL DISCUSSION

[After rolling the die for the final round of the game:] *Before we conclude with some wrap-up questions, I would like to thank you all for participating today. I know some parts of this game can be frustrating, especially when…* [Controller chooses whichever phrase is the most appropriate.]

- *…a well-conceived initiative fails due to the roll of a die,* OR
- *…a poorly conceived initiative succeeds due to the roll of a die.*

[Controller chooses to say this or not, based on all Devil's Advocate performances.] *Additionally, we recognize that the Innovator's position is a little more challenging. The Devil's Advocate has more time to think through what to say, and it's easier to point out the flaws in the Innovator's ideas. We purposely designed the game to encourage this type of interaction because it pushes players not only to identify potential ideas for preparing for the future, but also to think critically about how these ideas can be executed and in what timeframes they can be achieved, and to begin to address major risks.*

Although we've set up the game to encourage competition among players, it's important to stress that we are playing this game to generate ideas that will lead to more resilient and secure critical infrastructure systems in the future. I want to reiterate that it's your collective insights and subject matter expertise that matter. So, let's walk through what happened during each round today.

Walk through the outcomes of each round, and then move the game-board marker to its new position as follows:

- If all three initiatives pass in a round, move the marker up two positions.
- If two initiatives pass in a round, move the marker up one position.
- If one or no initiatives pass in a round, move the marker down one position.

Declare whether critical infrastructure systems have become more resilient as a result of the players' initiatives.

Some questions to ask during the open discussion include the following:

- What were your key takeaways?
- What was the most surprising or unexpected initiative presented?
- What was the most enjoyable part about playing the game? The least? Are there any improvements you would suggest?
- What would your organization do differently, given what was discussed during the game?

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?

Additional discussion questions

[These questions can be used to prompt the Innovator(s) if they get stuck or during the open discussion period following the die rolls. Facilitators can also tailor these questions or ask new ones to meet the matrix game sponsor's specific needs.]

- *What responsibility do the components of the ICT supply chain have in ensuring the security of data transmitted and stored using their hardware and software?*
- *Are there technological solutions that could help to mitigate against the use of personality profiles by malicious actors?*
- *What plausible steps can the Federal Government take to address weak security practices by the public and private sectors?*

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?

Additional discussion questions

[These questions can be used to prompt the Innovator(s) if they get stuck or during the open discussion period following the die rolls. Facilitators can also tailor these questions or ask new ones to meet the matrix game sponsor's specific needs.]

- *What responsibility do the components of the ICT supply chain have in ensuring the integrity of their hardware and software?*
- *What actions should be taken to ensure that other critical infrastructure sectors are not affected?*
- *What organizational or operational changes, if put in place prior to the incident, might have resulted in more effective prevention or faster resolution?*

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?

Additional discussion questions

[These questions can be used to prompt the Innovator(s) if they get stuck or during the open discussion period following the die rolls. Facilitators can also tailor these questions or ask new ones to meet the matrix game sponsor's specific needs.]

- *What actions could the United States take to ease the burden on the critical infrastructure sectors most likely to be impacted?*
- *What can the United States do to support the development of domestic sources of lithium?*
- *How could the United States prepare for a crisis scenario involving sudden restrictions on exports of processed lithium to the United States?*

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?

Additional discussion questions

[These questions can be used to prompt Innovator(s) if they get stuck or during the open discussion period following the die rolls. Facilitators can also tailor these questions or ask new ones to meet the matrix game sponsor's specific needs.]

- *What infrastructure could be installed to help alleviate reliance on groundwater?*
- *How can CISA and other government agencies better inform critical infrastructure owners and operators about climate risks?*
- *What plausible steps can the Federal Government take to protect critical infrastructure from water shortages? How might CISA contribute to this effort?*

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?

Additional discussion questions

[These questions can be used to prompt the Innovator(s) if they get stuck or during the open discussion period following the die rolls. Facilitators can also tailor these questions or ask new ones to meet the matrix game sponsor's specific needs.]

- *How should critical infrastructure owners and operators prepare for a future in which global internet governance has fragmented?*
- *What actions could the Federal Government take to address the failure of international consensus? What mitigating actions could be taken now to prepare for that future?*

APPENDIX VI: GAME SCHEDULE

Table 1: Schedule for conducting the Matrix Game

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