Secure Tomorrow Series

Alternative Futures: Brain-Computer Interfaces Controller Guide

Publication: August 2023
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 3 hours I will be your game controller for Alternative Futures: Brain-Computer Interfaces (BCIs). 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 (CI) 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 CI systems, and (2) identifies and analyzes the key indicators, trends, accelerators, and derailers associated with those risks to help CI 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 CI resilience and security in light of potential advancements in BCI technologies. 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 10–15 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 1. 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 CI owners increase the security and resilience of their systems in preparation of future issues that could arise from progress in and use of BCIs. Initiatives could be policies, legislation, 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 CI 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 1.] *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 2.] *As the Devil's Advocate, what is one reason why Player 1'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 1.] *Do you have a quick rebuttal?*

[Motion to Player 3.] *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

Brain-computer interfaces (BCIs) provide a direct communication pathway between the brain and an external device, for the purposes of either "reading" from or "writing to" the brain. Medical and military applications of BCIs—predominantly confined to laboratory settings—have been in development for decades. However, the field is currently undergoing a surge of interest and potential change in focus brought about by attention and investment from the private sector.

In the near term, potential applications of noninvasive BCI devices likely will be limited to read capabilities that include attention monitoring and mood detection. For the field to reach its full potential, researchers and developers will need to address following challenges:

- *Improve understanding of the human brain, including its processes and how to decode them.*
- *Overcome the trade-off between the signal clarity and more precise targeting of invasive BCI systems and the ease of use of noninvasive systems.*
- *Be able to read from and write to the brain in a way that is generalizable and requires little calibration.*
- *Establish broad consensus on ethical issues (neurodata[1] rights) and beneficial socioeconomic applications of this technology.*

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 CI during a plausible future scenario that could arise pertaining to BCIs. These scenarios may limit player actions, reflect new capabilities achieved through BCI technologies, or require players to consider the implications of an event. [Identify the first player to join the game 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

[1] Neurodata is commonly defined as any data generated through the nervous system.

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 1

As a reminder, for Round 1 you are considering initiatives that, if successfully begun today, you believe will help prepare CI owners for potential risks arising in these future scenarios.

[Turn to the Innovator(s).] *I am going to begin your turn by giving you 5 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 2 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 5 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 10–15 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 5 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 1. [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 1 winner.] *As the winner of Round 1, you get to choose the STEEP disruptor category for Round 2.*

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 1.

Declare the winner for Rounds 2 and 3 based on the results.

Direct the winning player or team to select a STEEP disruptor (Round 2 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 CI 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 CI 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?

APPENDIX I: SOCIAL DISRUPTOR

LAW ENFORCEMENT USE OF BCI CHALLENGES PRIVACY RIGHTS

BCI devices are slowly becoming a part of everyday life, just like the Internet did nearly four decades ago. A number of industries have adopted these devices to monitor employee attention, optimize operator control over systems, and increase safety. The general public has also adopted BCIs at growing rates. They are used much in the same ways that cell phones are used: for gaming and entertainment, personal organization and productivity, health monitoring, and communications. As of 2034, nearly 35 percent of Americans used a BCI device weekly, with 25 percent using it daily.

Use of data taken from BCIs by the public safety and law enforcement sector has been controversial, with a few cases making headlines and driving fierce public debate about privacy, defendant rights, and law enforcement overreach. Some examples include the following:

- *In 2033, police pressured a suspect in an assault case to wear a BCI during interrogations to record his unconscious reactions to stimuli, including a photo of the victim.*
- *In 2034, police confiscated an individual's BCI during a traffic stop and later charged him with impaired driving after allegedly reviewing the data stored locally on his BCI.*
- *In 2035, a whistleblower reported that available BCI data were often presented selectively in court, with prosecutors making dubious claims about what the neurodata revealed and with public defenders rarely having the time or resources to counter such claims.*

It is relatively uncontroversial for BCI data to be used similarly to how cell phone data have been used by investigators for decades—namely, for Global Positioning System (GPS) tracking and communications records. However, advocates for greater privacy protections argue that the use of BCI data crosses the line when it gives voice to a defendant's unvoiced opinions, memories, or responses to stimuli. These advocates point out that BCI data are difficult to interpret without a large amount of baseline data and that making inferences about an individual's recognition, inebriation, or emotional response is often speculative on the part of law enforcement.

What initiatives are necessary to protect the integrity and privacy of personal BCI data?

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.]

- *Are regulations necessary to balance public safety with law enforcement use of BCI capabilities while preserving individual privacy?*
- *Would there need to be new local or state-level data protection standards and policies? Would they have to match federal guidelines?*

- *What ethical considerations need to be considered when using BCI data for law enforcement and public safety?*

APPENDIX II: TECHNOLOGICAL DISRUPTOR

BCI DEVICES INTRODUCE NEW CYBER VULNERABILITIES

By 2037, BCIs are widely used to evaluate and assist workers in numerous industries, particularly ones that require rapid decision-making under pressure. BCIs successfully assist with employee monitoring, human-machine teaming, direct systems control, and decision-making.

In the air traffic control industry, air-traffic controllers wear electroencephalogram headsets that allow a supervisor or central command to monitor controllers, ensuring that employees who are fatigued or impaired are taken "off the floor." These noninvasive BCIs also adaptively manage workloads, funneling more difficult problems to employees who are displaying superior attention and vice versa. Additionally, the headsets are equipped with augmented reality glasses that help the air-traffic controllers access and process information more efficiently. Combined with growing levels of automation, BCIs have dramatically increased the safety and performance of the industry and enabled air traffic control services to meet increases in air traffic.

However, BCIs also create new vulnerabilities for the air traffic control industry, as evidenced by a cyberattack on the Sylvershelli Airport in July 2037. The attack occurred in stages, first causing a small number of the BCIs in operation to display faulty information to the controllers. This was followed by a "close-call" incident, which was mistakenly blamed on a trainee responsible for directing one of the planes. Finally, before the close-call incident could be investigated in detail, disaster struck as two passenger planes collided in mid-air.

A subsequent investigation revealed that although the airport's air-traffic control system was segmented from the internet, the BCI devices provided an entry point for malware.

What initiatives can you think of to improve the cybersecurity of BCI devices, while not overly impeding their functionality?

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 protections should be placed on BCI systems to prevent malicious cyberactivity? What cybersecurity considerations should the aviation industry and other CI sectors consider to mitigate the potential risk from BCI devices?*
- *How should the potential benefits of BCI systems be weighed against the risks in the aviation industry and other CI sectors?*
- *How might cybersecurity needs differ for BCI devices versus other systems and technologies that allow users to interface with the internet?*
- *Are there any industries or sectors that should not implement BCI-based systems?*

APPENDIX III: ECONOMIC DISRUPTOR

NEW ATTENTION-MONITORING REGULATION SHUTS DOWN SUPPLY CHAINS

A comprehensive study released in 2030 shows that new BCI attention-monitoring devices greatly reduce truck driver-caused accidents. As a result, federal mandates were proposed for all long-haul commercial truck drivers to use these devices by 2033. Under the new regulation, commercial drivers must continuously wear a BCI headset while their vehicles are in motion.

- *If the device detects that a driver's attention is drifting from the road or the driver is otherwise sleepy or impaired, it first gives the driver a warning.*
- *If the driver's attention does not increase within 5 minutes, the device warns the driver to pull over at the next available rest stop, and a GPS device in the cab indicates the location of the next safe stop to the driver.*
- *Drivers who: are persistently inattentive, sleepy, or impaired while driving; remove the BCI devices; or ignore warnings to pull off the road can face fines, penalty points, and ultimately revocation of their commercial driver's license.*

Most long-haul truck drivers nationwide vehemently oppose the proposed regulation, as do many smaller trucking companies. Critics of the regulation point to the fact that driver hours behind the wheel are already strictly regulated with mandatory rest breaks. They are particularly concerned that these devices will collect months of data on driver attention levels, violating truckers' constitutional right to privacy. In contrast, federal officials say that the data are only stored locally in the cab. While officials acknowledge that data will periodically be uploaded from drivers' cabs for research purposes, they have sought to assure drivers and companies that this data will be thoroughly anonymized and its usage is subject to strict safeguards.

In 2033, as the regulation is set to go into effect, numerous trucking associations stage a nationwide, First Amendment–protected, peaceful protest against the BCI regulation. Convoys involving thousands of trucks blockade interstates, bridges, and ports. Other drivers go on strike, leading to disrupted supply chains and product shortages nationwide. After a few days, gas stations have run out of fuel, hospitals are short on medical supplies, supermarket shelves are bare amid panic buying, and traffic jams persist at key chokepoints along interstates.

What initiatives can you think of to balance the privacy concerns expressed by the truck drivers with the increased safety resulting from the use of BCI devices?

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 government agencies have in developing and supporting risk mitigation strategies that balance public safety and individual privacy?*
- *What initiatives could address workplace concerns about privacy more broadly when BCI technologies are introduced to monitor workers in other contexts (e.g., distribution center employees, air traffic controllers)?*

APPENDIX IV: ENVIRONMENTAL DISRUPTOR

NEW OPPORTUNITIES FOR BCI CAPABILITIES IN EMERGENCY SERVICES

The country of Fictitia is making a splash for what some news commentators and pundits are calling "the most successful government-led emergency response effort in history." Following a devastating 7.9 magnitude earthquake and subsequent landslide in Fictitia on September 16, 2035, Fictitia spokespersons highlighted their use of BCI applications that they claimed would revolutionize emergency response. Some of the reported capabilities include the following:

- *BCI-optimized surveillance drones and robots, which are facilitating search and rescue in remote, dangerous, or inaccessible areas*
- *BCI-enhanced coordination, monitoring, and support for responders, including cognitive and physical performance monitoring, supporting decision-making by feeding information to responders, and one-on-one and team brain-to-brain communication channels between responders*
- *BCI-controlled search and rescue dogs*

U.S. experts long suspected that Fictitia had been testing and implementing BCI applications among its special operations forces but were surprised by their reported use in the emergency response. Initial skepticism at Fictitia's claims quickly dissolved as the rescue operations unfolded, giving way to criticisms as to why responders in the United States lack access to these capabilities. Barriers mentioned include the high cost for most local agencies, infrastructure requirements, and security concerns.

How can BCIs be implemented effectively in the U.S. Emergency Services sector?

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 challenges may arise in implementation? Which, if any, challenges are unique to this sector? Alternatively, what other barriers to implementation might be encountered in other CI sectors?*
- *What hardware and infrastructure requirements will need to be met and how can those needs be met in remote or damaged areas?*
- *How should cybersecurity be maintained in a challenging environment where accessibility is highly prioritized?*

APPENDIX V: POLITICAL DISRUPTOR

FOREIGN DATA COLLECTION ON U.S. CITIZENS

By the mid-2030s, BCIs have become more commercially available, more advanced, and more widely used in a number of professions. With their increase in popularity have also come attempts to mine brainwave data. Reading a person's mind is still out of reach—neurodata are still too "noisy" for nuanced interpretations, such as what a person is thinking. However, mining efforts can reveal emotional responses, responses to stimuli, mental patterns, and sensitive health information. When combined with big data analytics, neurodata may offer insights into the mental and neurological health and habits of Americans, which may offer economic insights or security advantages to foreign adversaries.

Foreign adversaries are stockpiling neurodata, which suggests they are investing in the analytic capabilities to harness neurodata. One country has already poured billions of dollars into BCI research, drawing on massive amounts of data from countries around the world to aid in their research efforts. Analysts worry that foreign adversaries will use the accumulated data to advance their artificial intelligence capabilities and their understanding of the human brain, enabling them to decode the neuro "noise" to glean new and potentially dangerous insights.

In 2036, Raven, Inc., a technology company that produces BCIs for several branches of the U.S. military, is criminally hacked. Although the company claims that minimal information was stolen and that no military data was accessed, many cyber experts suspect that Raven is downplaying the extent of the intrusion. Regardless, the criminal hack has raised concerns about how this stolen data could be used against U.S. military personnel.

What actions should the United States take to mitigate against potential future risks from foreign adversaries mining BCI data?

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 special protections, if any, should be afforded to neurodata?*
- *Do the potentially significant insights that can be learned from neurodata represent an unacceptable security risk to the United States? If so, what can be done about it?*

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)	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 CI security and resilience (Controller)	5 Min	20 Min Total
	- Open discussion period (Players)	15 Min	