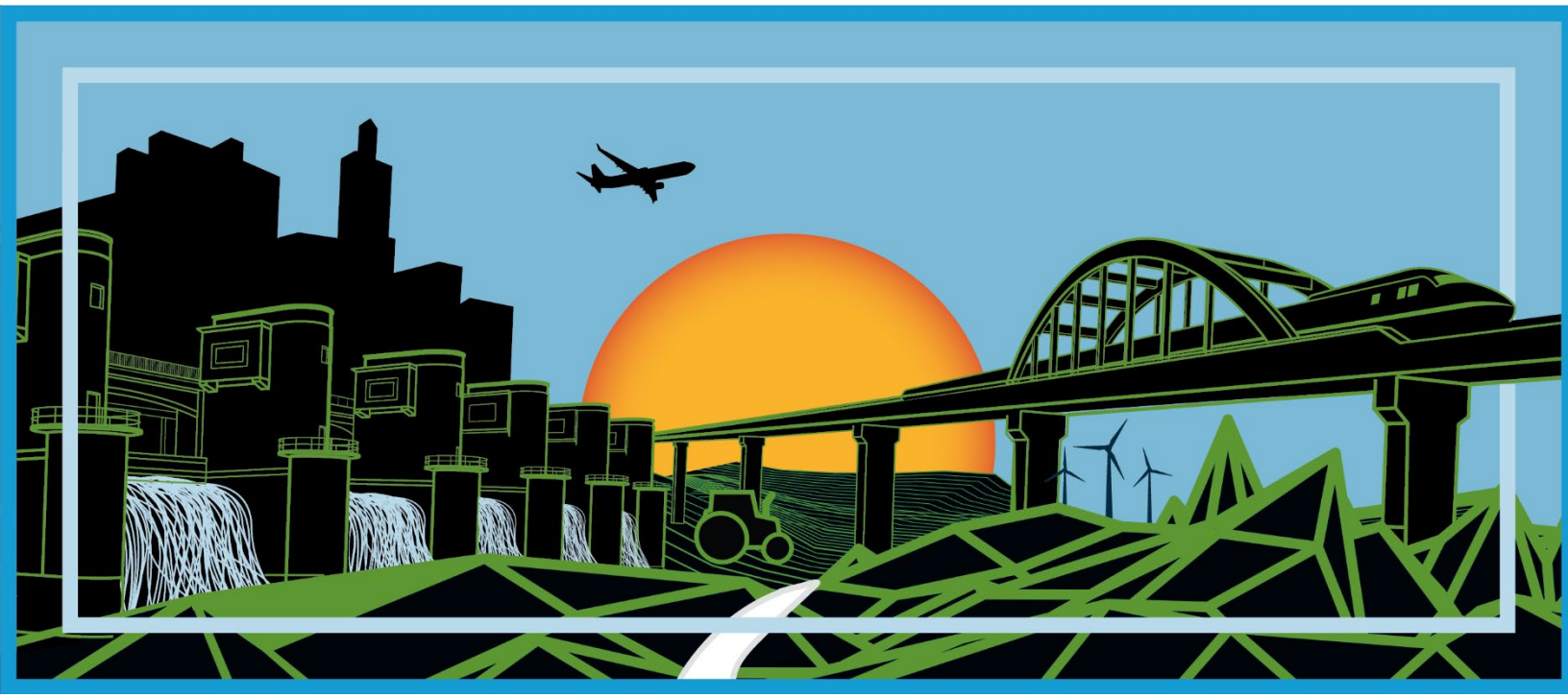

Secure Tomorrow Series

Alternate Futures: Brain-Computer Interfaces Players Guide

Publication: August 2023
Cybersecurity and Infrastructure Security Agency

BACKGROUND

How prepared are critical infrastructure (CI) sectors in light of potential advances in brain-computer interface (BCI) technologies? *Alternative Futures: Brain-Computer Interfaces* presents you with scenarios that could plausibly occur within the next 10–15 years. During each round, you and your opponents will take turns proposing initiatives and debating strategies that will shape CI resilience and security in light of potential advancements in BCI technologies. 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 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.

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 3 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 CI resilience and security in light of potential advancements in BCI technologies. 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 CI 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 the usage and implementation of BCI devices?

- What are the implications for future CI resilience and security?
- Are there specific ramifications for one or more CI sectors?
- Is there a role for CISA to address threats and uncertainties associated with the usage and implementation of BCI devices?
- Are there other trends that may influence the potential advancements in BCI technologies?

PRESENT STATE

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.

PLAYING THE GAME

Alternative Futures: Brain-Computer Interfaces has three rounds, each of which will present the players with a scenario that could plausibly occur within the next 10 to 15 years. In Round 1, the Innovator(s) will have 15 minutes to identify up to three initiatives that will support CI 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 5 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).

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

- 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 2 and 3, 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; an election outcome is a potential political disruptor that could affect funding for CI projects; cyberattacks are a technological disruptor with a wide range of cascading implications for all CI sectors.

To account for a changing future environment, each round features a STEEP disruptor scenario that may limit player actions, alter the trajectory of current trends in BCI technologies, 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 CI security and resilience (Controller)	5 Min	20 Min Total
	-	Open-discussion period (Players)	15 Min	

Participants are reminded that any information shared during this game is provided on a voluntary basis. Sensitive information, to include confidential or proprietary information, should not be shared. Information shared during this game may be recorded for the purposes of facilitating the program and discussions. However, discussion or disclosure of information in these sessions is not a substitute for submission under the Protected Critical Infrastructure Information Program. Therefore, information may be subject to Freedom of Information Act requests or other mechanisms that would publicize any information shared or recorded.

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.

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?

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 Sylvershelli International 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 improve the cybersecurity of BCI devices, while not overly impeding their functionality?

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 these data will be thoroughly anonymized and their usage 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 balance the privacy concerns expressed by the truck drivers with the increased safety resulting from the use of BCI devices?

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?

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 were accessed, many cyber experts suspect that Raven is downplaying the extent of the intrusion. 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 potential future risks from foreign adversaries mining BCI data?