ALTERNATIVE FUTURES: DATA PRIVACY, STORAGE, AND TRANSMISSION CONTROLLER GUIDE

Secure Tomorrow Series

WELCOME AND INTRODUCTIONS

Hello. My name is [name], and for the next three hours I will be your game controller for Alternative Futures: Data Privacy, Storage, and Transmission[1]. 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 National Risk Management Center has developed this game as part of a broader effort by the Cybersecurity and Infrastructure Security Agency (CISA) to plan strategically for its future operating environment. The long-term goal of this project 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.

A key part of this effort is obtaining knowledge and perspectives from a diverse group of stakeholders and subject matter experts. 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 data privacy, storage, and transmission trends. 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 5 to 10 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.* [Note: Depending on the number of players, there could be one Innovator or a team of up to three Innovators.] *During the first round,* [assign which player has what role for Round 1]. *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 trends and expectations regarding data privacy, storage, and transmission. These 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 critical infrastructure sectors for the future. You will have 15 minutes to think of and present up to three initiatives, as well as up to three supporting arguments per initiative. When proposing an initiative, please take into consideration both its potential impact 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.]
- ***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 describe 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*

[1] *Alternative Futures: Data Privacy, Storage, and Transmission* combines two Secure Tomorrow Series topics: Anonymity and Privacy and Data Storage and Transmission.

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, environmental, economic, 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 by listening to both sides and determining whether an initiative 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/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. Your collective subject matter expertise will be represented in our final products, regardless of the outcomes of each round.*

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 example using a completely unrelated topic. As the topic, let's use "reducing obesity in the United States."

[Motion to Player 1.] *What is one initiative that you think might help reduce obesity nationwide? Now, provide a supporting argument why you think that this initiative would be successful, considering both how the initiative would affect obesity 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 Player1'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 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 ultimately is 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

For years now, companies have been increasingly monetizing data, with data promising to unlock the potential for artificial intelligence (AI) to predict and even shape human behavior. Users are required to share personal data with organizations to receive useful services and personalized products. Several emerging trends are contributing to a loss of anonymity and privacy and an increasingly insecure landscape for data storage and transmission:

1. *The monetization of data has created an unregulated market for user data—a Wild West where so-called third-party data brokers[2] have amassed significant amounts of data at the individual level. For example, Oracle claims to have data on 80% of the U.S.'s internet-using population, with over 30,000 data attributes per user.[3]*
2. *Anonymity has been lost. Although organizations have been de-identifying datasets to avoid personal data concerns,[4] numerous cases have shown that advances in machine learning, artificial intelligence, and supercomputers are enabling reidentification of users through the "mosaic effect."[5]*

[2] Margaret Levi (Director, Center for Advanced Study in the Behavioral Sciences; Professor of Political Science, Stanford University), interview with STS team, August 19, 2020.
[3] Aliya Ram and Madhumita Murgia, "Data Brokers: Regulators Try to Rein in the 'Privacy Deathstars'," Financial Times, January 8, 2019, https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.
[4] Adam Hill (Director, Gartner, Legal, Compliance & Privacy Research, Gartner), interview with STS team, September 11, 2020.
[5] Natasha Lomas, "Researchers spotlight the lie of 'anonymous' data," Tech Crunch, July 24, 2019, https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?renderMode=ie11; and Alex Hern, "'Anonymised' data can never be totally anonymous, says study," The Guardian, July 23, 2019, https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds.

3. *With a growing consumer digital footprint, data from third-party cookies,[6] location services,[7] "fingerprinting,"[8] and pre-built user profiles[9] allow interested parties to follow users across platforms, micro-target users, and tailor disinformation campaigns.[10]*
4. *The global data sphere is projected to triple over the next 5 years from 59 Zettabytes in 2020 to 175 Zettabytes by 2025.[11] Meanwhile, larger data volumes are contributing to a shift toward a greater reliance on public cloud-storage providers.[12]*
5. *Many countries are taking action to ensure control over national data by prohibiting transfers of data out of the country or by seeking to limit foreign access to certain kinds of data, and sometimes go as far as controlling and limiting content dissemination online. Data localization will greatly slow or prevent the flow of data worldwide, increasing private sector costs, enabling foreign adversaries to hoard data, and limiting the ability of U.S. firms to innovate.*

Within the U.S., companies are struggling to comply with a patchwork of state data privacy regulations.[13] In an evolving privacy landscape, the International Association of Privacy Professionals' (IAPP) has developed a table to keep track of state-level privacy legislation. For information on which states have proposed and enacted comprehensive privacy bills, visit: https://iapp.org/resources/article/state-comparison-table/.[14]

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, environmental, economic, 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 from further erosion of trust and social cohesion. These issues may limit player actions, alter the trajectory of current trust and social cohesion trends, 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.]

---

[6] Federal Trade Commission, "Online Tracking," last accessed September 4, 2020, https://www.consumer.ftc.gov/articles/0042-online-tracking.
[7] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," The New York Times, December 10, 2018, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[8] Fingerprinting is the improved online tracking version of the cookie, collects specific information about the user's devices such as screen resolution, model, operating system, etc. that cannot easily concealed or changed to track users online; Brian X. Chen, "'Fingerprinting' to Track Us Online Is on the Rise. Here's What to Do.," The New York Times, July 3, 2019, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[9] Craig Timberg, "Critics say Facebook's powerful ad tools may imperil democracy. But politicians love them.," The Washington Post, December 9, 2019, https://www.washingtonpost.com/technology/2019/12/09/critics-say-facebooks-powerful-ad-tools-may-imperil-democracy-politicians-love-them/.
[10] Jim Lewis (Director, Center of Strategic and International Studies), interview with STS team, September 15, 2020.
[11] David Reinsel, John Gantz, and John Rydning, Data Age 2025: The Digitization of the World from Edge to Core (November 2018), IDC, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
[12] Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction (New York: Rosetta Books, 2019).
[13] Michael Beckerman, "Americans Will Pay a Price for State Privacy Laws," The New York Times, October, 14, 2019, https://www.nytimes.com/2019/10/14/opinion/state-privacy-laws.html.
[14] Mitchell Noordyke, "U.S. State Comprehensive Privacy Law Comparison," IAPP, last accessed September 4, 2020, https://iapp.org/resources/article/state-comparison-table/.

LET'S PLAY

Round 1

As a reminder, for Round I, you are considering initiatives that, if successfully begun today, you believe will help prepare critical infrastructure owners for potential risks to data privacy, storage, and transmission 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.*

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 his or her first initiative.]

Try to have the Innovator frame arguments by explaining:

- How his or her 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 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 5 to 10 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 round, or after 15 minutes, recap the Innovator 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 his or her 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 to begin his or her rebuttal, and start the timer.

After the rebuttal period, ask the Judge to select the likelihood of success for each initiative and to present his or her 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 (< 10 minutes) following judgment to continue this discussion.]

[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/team to select a STEEP disruptor (Round 2 only).

WRAPPING UP AND FINAL DISCUSSION

[After rolling the die for Round 3 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.*

I want to reiterate that we have documented all of the ideas discussed today, and it's your collective insights and subject matter expertise that will be represented in our final products.

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. 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?

APPENDIX I: SOCIAL DISRUPTOR

1. INCREASED NUMBER OF EMPLOYEES TELEWORKING

At one point during the 2020-21 COVID-19 pandemic, more than one-third of employed U.S. adults were teleworking, including more than 56 percent of government workers. Over the next five years, the percentage of the U.S. workforce with remote-work arrangements has continued to grow significantly. By 2025, more than 50 percent of U.S. organizations have shifted at least some portion of their employees to remote work permanently, particularly within local, state, and federal government agencies and tech-related industries. For example, almost half of Facebook employees continue to work remotely and two-thirds of government employees spend a minimum of 20 hours a week working remotely.

Increased telework has prompted organizations to reevaluate required data structures to support the needs of remote workers and increase their resilience. With increased demand for remote access comes increased risk, and examples abound of employees accessing sensitive data inappropriately or connecting to networks without following appropriate security protocols. Malicious actors have seized on security vulnerabilities associated with remote work, leading to several high-profile examples of data breaches and cybersecurity incidents:

- *In 2023, malware operators launched sophisticated spear-phishing attacks targeting teleworkers to steal their usernames and passwords and gain access to sensitive data within their organizations' networks. One breach at a popular social media company exposed the personal information of more than 100 million people, which were sold to spammers and used to develop targeted financial scams and other spear-phishing attempts. An internal investigation revealed that the company did not use multi-factor authentication (MFA) for remote access. A Justice Department investigation indicates that a Chinese government-linked hacking group was behind the attack.*
- *In 2024, hackers gained access to numerous public and private organizations through a compromised virtual private network (VPN) software update that opened users up to a common hack, known as a "man in the middle" attack, which allows an unauthorized third party to see everything the user is doing and/or redirect them to a malicious server. The FBI traced the VPN software hack to a cybercrime organization.*

Considerations

What initiatives are necessary to account for security risks and vulnerabilities to data security as remote work continues to increase?

- *What additional actions should be taken to support efforts by owners and operators to secure critical infrastructure from cyberattacks targeting remote operations?*
- *What plausible steps can the federal government take to address weak security practices by the public and private sectors? How might CISA specifically contribute?*

2. SOCIAL CREDIT SYSTEM

U.S. data brokers have consolidated from a few hundred into the "Big Five" and it's become standard practice to engage their services. Reminiscent of China's social credit system,[15] these agencies run background checks on people's financial fitness, employment history, political affiliations, webpages frequently visited, and closest social connections for all manner of applications, including supporting investigations by law enforcement agencies. U.S. government agencies have also begun to contract with these agencies to revamp security clearance programs.

The vast amount of data stored with data brokers makes them prime targets of cyberattacks from state or non-state actors. The Big Five have repeatedly assured customers and the U.S. government that systems are in place to mitigate risks. However, two recent examples highlight their continued vulnerabilities:

- *In 2023, malware operators launched sophisticated spear-phishing attacks on Big Five employees. One breach exposed the personal information of more than 100 million people, which was sold to spammers and used to develop targeted financial scams and other spear-phishing attempts. A Justice Department investigation indicates that a Chinese government–linked hacking group was behind the attack.*
- *In 2024, the FBI uncovered a plot in which a disgruntled employee was offering to sell classified security clearance data to foreign governments. Investigations revealed multiple security vulnerabilities and weak access control practices within the company.*

Considerations

What initiatives are necessary to protect the integrity and privacy of personal data under a system in which data broker services are highly sought after by individuals, corporates, and government agencies?

- *How should you support efforts to achieve the right balance between preserving privacy and benefiting from this data?*
- *What plausible steps can the federal government take to enhance privacy protections from data brokers offering social credit system services? How might CISA specifically contribute?*

[15] See https://www.wired.com/story/is-big-tech-merging-with-big-brother-kinda-looks-like-it/

APPENDIX II: TECHNOLOGICAL DISRUPTOR

CYBERATTACKS THROUGH EDGE DEVICES

A growth area of the Internet of Things (IoT) are edge devices, which store and process data locally to minimize the delays inherent in sending data back and forth from the cloud. By 2025, the U.S. market for edge hardware has reached $200 billion.

Unfortunately, these devices come with their own cybersecurity concerns. Edge devices are often poorly protected and positioned at the boundaries of interconnected networks, and they dramatically increase the attack surface. Cybersecurity attacks on edge devices can be difficult to detect; IT administrators rarely engage in the detailed level of network traffic monitoring necessary to do so. Bad actors can string together many edge devices and take advantage of their processing power to conduct cyberattacks.

Three recent cyberattacks illustrate some of the security weaknesses:

- *A major pharmaceutical manufacturing company was using edge devices to track its equipment levels and perform predictive maintenance. Its fleet of 30,000 edge devices—split between several factories and transport vehicles—were infected by a virus that uses the network for cryptocurrency mining. As a result, the processing speed of all these devices slowed to a crawl. Because of how the devices communicate with each other, the virus proves technically infeasible to remove and the company is forced to replace its entire fleet of devices.*
- *In 2024, a major virus, using Mirai source code, strung together hundreds of thousands of unsecured, internet-connected edge devices to launch a distributed denial-of-service (DDoS) attack on a major internet service provider lasting for a shocking seven days. More broadly, the growing number of edge and IoT devices has doubled the number of DDoS attacks globally from 7.9 million in 2018 to 15.4 million in 2023.*
- *An auto manufacturer's "smart" assembly plant was shut down for several hours when a ransomware attack locked all of the robotic devices on the factory floor. The manufacturer paid the ransom—approximately $100,000 in bitcoin—to have its devices unlocked.*

Considerations

What initiatives can you think of to address cybersecurity threats faced by critical infrastructure owners and operators as use of edge devices increases?

- *Are you aware of any industries or critical infrastructure sectors that have or are likely to invest in edge computing? How does the risk differ from edge devices versus IoT sensors? What possible consequences might occur from a cyberattack?*
- *As edge computing takes off, what initiatives can be put in place to mitigate current concerns about cyber vulnerabilities associated with edge devices?*
- *What knowledge gaps might CISA address to assist critical infrastructure owners on the security implications of implementing an edge-device architecture for data collection and processing? How can the federal government best assist critical infrastructure owners on this issue?*

APPENDIX III: ECONOMIC DISRUPTOR

BALANCING PROTECTIONS FOR CORPORATE INSIDER INFORMATION AND EMPLOYEE PRIVACY

In the years following the COVID-19 pandemic, U.S. and European economies are mired in a prolonged recession, with several major multinational corporations having filed for bankruptcy. In 2023, security experts recognized a disturbing trend where competitors, foreign governments, and other nefarious actors use micro-targeting tactics to identify vulnerable employees of failing companies who may be willing to sell insider information, including data, prediction models, and trade secrets. In light of this, companies started implementing employee sentiment and activity monitoring programs. These programs track employee online behavior—both inside and outside the office—for potentially suspicious behavior to identify insider threats.[16] Companies using these programs tout that they are mitigating threats by tracking employee spending habits, web searches, and social medial connections. One notable example in 2024 involved a defense contractor who offered to sell schematics for the Navy's next-generation attack submarine to an undercover FBI agent. However, employees, unions, and advocacy groups like the ACLU are raising privacy concerns.

Considerations

How should you support critical infrastructure partners' efforts to achieve the right balance between preserving the security of their intellectual property and their employees' expectations for privacy?

- *How could CISA and federal agencies better support critical infrastructure owners in their efforts to balance employee data privacy and potential security risks?*
- *How could critical infrastructure owners mitigate concerns and possible backlash—both internal and external to their organizations—from implementing sentiment analysis?*
- *What ethical considerations need to be taken into account when implementing an employee sentiment and activity monitoring program? What bodies and actors are best suited to address these considerations?*
- *Are there systemic risks introduced by allowing individual companies to decide whether or not to conduct a sentiment and activity monitoring program? How might federal agencies mitigate some of these risks while retaining the advantages of these programs?*

[16] See https://www.gartner.com/smarterwithgartner/the-future-of-employee-monitoring/ and https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy

APPENDIX IV: ENVIRONMENTAL DISRUPTOR

DATA CENTER OPERATIONS

Extreme weather is increasing across the U.S.: "arctic bombs" in the North and Northeast, hurricanes and storm surge along the East Coast and the Gulf, flooding in the Midwest and Great Plains, wildfires on the West Coast, and heatwaves in the South and Southwest. The ongoing barrage of natural hazards has become a significant threat to data storage centers, which have to deal with both damage to their facilities and interruption of their power supplies.

- *Flooding, fire, and other hazards have damaged facilities and permanently destroyed data, most notably in California when the wildfires of 2023 led to the shutdown of 13 data centers near Sacramento. Hurricane Mindy in 2021 caused flooding of two data centers in Charleston, South Carolina, and Hurricane Helene in 2024 swamped five data centers in the Jacksonville, Florida, area.*
- *Power and water interruptions not only prevent access to data, but also can lead to overheating in facilities. In 2022, a heatwave in eastern Texas caused a two-day blackout and 33 data centers experienced at least a partial shutdown.*

Further, as observed in the aforementioned Texas example, data centers tend to cluster in hubs and any hazard that can impact one of them often impacts several. Lastly, given the range of data that can be housed in a data center and the way data is often split between facilities, it's proven difficult to predict what or who will be impacted by a data center going off-line.

Considerations

What initiatives can you think of to safeguard access to data housed at data centers at risk from water and electrical interruptions and other damages from wildfire, high wind, high temperatures, and rising sea-levels?

- *How can you support critical infrastructure partners in becoming more informed about vulnerabilities to data centers and potential risks to the data housed there?*
- *What plausible steps can the federal government take to safeguard data housed in data centers? How might CISA specifically contribute?*

APPENDIX V: POLITICAL DISRUPTOR

1. LACK OF NATIONAL PRIVACY LEGISLATION

In 2024, the European Court of Justice rules that the U.S. cannot be trusted as a safe destination for transferring, storing, or processing EU citizen data. In light of this ruling, U.S. organizations are now scrambling to figure out how to identify and separate the data of EU citizens and make alternative storage arrangements. Additionally, since diversifying datasets is key to developing better algorithms and training them, having EU data is absolutely crucial for U.S. AI research and development efforts. Without this data, the U.S. risks falling behind to competitors like China.

Considerations

What initiatives can you think of to mitigate the effects of differing legislation and requirements between the U.S. and the EU for data transferring, storage, or processing?

- *Would this scenario lead to further implications for data storage, processing, and transfer with other countries)?*
- *What plausible steps can the federal government take to support critical infrastructure partners' efforts to comply with EU requirements without sacrificing AI research and development? How might CISA specifically contribute?*
- *What provisions might need to be added to a U.S. version of data privacy legislation?*

2. FRACTURING GLOBAL INTERNET

Following trends in digital sovereignty and as a reflection of India's own nationalist movement, Indian Prime Minister Narendra Modi, after claiming a third term in 2024, declares that India will segment its internet from the global internet as a matter of "Indian national security." India will follow China's "Great Firewall" model, which famously employs filters to selectively block certain internet sites, words, IP addresses, and so on. Further, all data on Indian citizens must be stored in India.

The growing fragmentation of the internet is problematic for the Border Gateway Protocol, which is the global navigation system that manages the flow of data around the world. Incompatibility between web services, communication standards, and hardware devices are causing a growing number of problems with information routing, with potentially severe effects on international businesses. For instance:

- *A routing error caused all traffic to a popular music streaming site to be temporarily routed to a small Pennsylvania construction company's website for almost an hour.*
- *Large chunks of network traffic belonging to MasterCard, Visa, and more than two dozen other financial-services companies were routed briefly through a Russian telecom, exposing millions of customers' personal and financial data.*
- *An international shipping company found that a problematic latency in its data traffic, which was impacting its operations, was caused by malicious rerouting of internet traffic.*

Considerations

How should critical infrastructure owners and operators prepare for a future in which international data and transmission protocols are less readily available or not available at all?

- *What actions could CISA and the federal government take to address the failure of international protocols for managing data transmission? What mitigation actions could be taken now to prepare for that future?*
- *The global trend towards cyber sovereignty is driven by a combination of concerns about U.S. surveillance, digital colonialism, being trapped between China and the U.S.'s great-power politics, protectionism for domestic industries, and genuine concerns about security risks inherent in the global internet model. What can CISA and the federal government do to increase faith in the global internet and reduce the temptation to opt-out?*

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) - Present counterarguments (Devil's Advocate) - Rebuttal (Innovator) - 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) - Present counterarguments (Devil's Advocate) - Rebuttal (Innovator) - 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) - Present counterarguments (Devil's Advocate) - Rebuttal (Innovator) - 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