however, 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 STEEP and 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 and 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

Social cohesion is commonly defined as citizens' belief that they share a moral community or common focus on social wellbeing with one another, their governing bodies, and other institutions. Institutions, including government agencies, can act in ways that increase cohesion, or ways that worsen the "cleavages of class, race, religion, national origin, and culture" and divide society.[1] Social science research has found that repeated "failures" by institutions to deliver on promises—such as a police force that continues to engage in brutality—can significantly harm public trust.[2] A lack of accountability and transparency in public governance also negatively affects public trust.[3] Public trust can wane because a government or infrastructure sector is perceived to be untrustworthy or ineffective in fully mitigating risks (e.g., significant data breaches, disaster responses failures).[4] The public can begin to lose trust because of exposure to convincing sources of misinformation (e.g., anti-vaccination sentiment because of celebrity promotion of inaccurate information on social media[5]).

Current social divisiveness presents numerous opportunities for malicious actors to diminish trust in public institutions. Disinformation—augmented through the access provided by social media platforms—can push a significant fraction of individuals to become impenetrable to evidence-based arguments, presenting a potential danger to themselves and others and to an effectively functioning democracy. For example, algorithms underlying customized searches and personalized social media are generating echo chambers, exacerbating confirmation bias and contributing to the radicalization of identity-driven groups.[6][7][8] Individuals and groups can easily push information (factual or not)

---

[1] Norman C. Capshaw, "The Social Cohesion Role of the Public Sector," *Peabody Journal of Education* 80, no. 4 (2005): 53–77.
[2] Margaret Levi (Director, Center for Advanced Study in the Behavioral Sciences; Professor of Political Science, Stanford University), interview with STS team, Aug. 19, 2020.
[3] Heinrich Kroukamp, "Strategies to Restore Confidence in South African Local Government," *African Journal of Public Affairs* 9 (2016): 105-116.
[4] Norman C. Capshaw, "The Social Cohesion Role of the Public Sector," *Peabody Journal of Education* 80, no. 4 (2005): 53–77; and Margaret Levi (Director, Center for Advanced Study in the Behavioral Sciences; Professor of Political Science, Stanford University), interview with STS team, Aug. 19, 2020.
[5] Richard A. Stein, "The Golden Age of Anti-Vaccine Conspiracies," *Germs* 7, 4 (2017): 168–170.
[6] National Intelligence Council, *Global Trends Paradox of Progress* (Jan. 2017), https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf; Christopher Seneca, "How to Break Out of Your Social Media Echo Chamber," *Wired*, Sept. 17, 2020, https://www.wired.com/story/facebook-twitter-echo-chamber-confirmation-bias/.
[7] Confronting the Rise of Domestic Terrorism in the Homeland, Before the House Homeland Security Committee, 116th Congress (May 8, 2019) (statement of Michael C McGarrity, Assistant Director, Counterterrorism Division, FBI), https://www.fbi.gov/news/testimony/confronting-the-rise-of-domestic-terrorism-in-the-homeland.
[8] National Intelligence Council, *Global Trends Paradox of Progress* (Jan. 2017), https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf.

representing wide-ranging and divergent topics and messages out to a large audience,[9] presenting a growing signal-to-noise challenge for identifying credible threats.[10]

Once trust is lost, a wide range of drivers for public skepticism makes it difficult to design and implement initiatives promoting public trust. For example, the public's skepticism of nuclear power is not driven by a singular viewpoint. Some do not trust the technology, some do not trust the government or industry's ability to manage nuclear power risks, some view it to be overly damaging to the environment, and others recall nuclear power plant incidents or near-incidents (e.g., Chernobyl, Fukushima Daiichi, and Three Mile Island).[11]

Finally, supply chains—including those critical to the sustained operations of U.S. critical infrastructure sectors (e.g., healthcare and public health sector, energy sector, information technology sector)—have become increasingly global.[12] Trust in the collaborative relationships within supply chains are critical for both end users and entities operating within these chains, and any imbalances could have serious consequences to maintaining operational performance.[13] By owning or operating critical supply chain nodes around the globe, China in particular could hold up maritime trade flows and therefore presents an increasing challenge to maintaining U.S. trust in global supply chains.

Select a STEEP disruptor

[Point to the STEEP and 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.]

---

[9] Janna Anderson and Lee Rainie, *Many Tech Experts Say Digital Disruption Will Hurt Democracy* (Feb. 2020), Pew Research Center, https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/; and Seth Flaxman, Sharad Goel, and Justin M. Rao, "Filter Bubbles, Echo Chambers, and Online News Consumption," *Public Opinion Quarterly* 80, iss. S1 (2016): 298–320.

[10] Janna Anderson and Lee Rainie, *Many Tech Experts Say Digital Disruption Will Hurt Democracy* (Feb. 2020), Pew Research Center, https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/.

[11] Rose G. Campbell, "A Content Analysis Case Study of Media and Public Trust in Japan: After the Quake," *Observatorio (OBS*) Journal* (2019): 131–147; Guizhen He, Arthur P.J. Mol, Lei ZZhang, and Yonglong Lu, "Nuclear Power in China after Fukushima: Understanding Public Knowledge, Attitudes, and Trust," *Journal of Risk Research* 17, iss. 4 (2014): 435–451; James Flynn, "Public Trust and the Future of Nuclear Power," *Energy Studies Review* 4, no. 3 (1992): 268–277; Michael Greenberg and Heather B. Trulove, "Energy Choices and Risk Beliefs: Is It Just Global Warming and Fear of a Nuclear Power Plant Accident?," *Risk Analysis* 31, no. 5 (2011): 819–831; Rebecca Riffkin, "For the First Time, Majority in U.S. Oppose Nuclear Energy," Gallup, Mar. 18, 2016, https://news.gallup.com/poll/190064/first-time-majority-oppose-nuclear-energy.aspx; RJ Reinhart, "40 Years After Three Mile Island, Americans Split on Nuclear Power," Gallup, Mar. 27, 2019, https://news.gallup.com/poll/248048/years-three-mile-island-americans-split-nuclear-power.aspx.

[12] Supply Chain Resiliency: Hearing before the U.S. House of Representatives Committee on Small Business Subcommittee on Economic Growth, Tax, and Capital Access, 116th Cong. 1-5 (2020) (testimony of Eswar S. Prasad); and Barthélémy Bonadio, Zhen Huo, Andrei A. Levchenko, and Nitya Pandalai-Nayar, "Global Supply Chains in the Pandemic," *National Bureau of Economic Research Working Paper 27224* (May 2020), https://www.nber.org/papers/w27224.pdf.

[13] Peter M. Ralston, R. Glenn Richey, and Scott J. Grawe, "The Past and Future of Supply Chain Collaboration: A Literature Synthesis and Call for Research," *International Journal of Logistics Management* 28 (2017): 508-530; and Mohammad Asif Salam, "The Mediating Role of Supply Chain Collaboration on the Relationship between Technology, Trust and Operational Performance, An Empirical Investigation," *Benchmarking: An International Journal* 24 (2017): 298–317.

APPENDIX I: SOCIAL DISRUPTOR

CONSPIRACY THEORIES

Over the next five years, personalized networking, microblogging, and video-sharing social media platforms continue to facilitate social divisiveness and the radicalization of like-minded groups. The spread of disinformation—representing wide-ranging and divergent topics—continues with relatively few checks and limitations. Social media groups act as echo chambers and reinforce the growth and longevity of conspiracy theories, many of which have harmful and damaging consequences. For example:

In 2021 and 2022, conspiracy theories related to COVID-19 were rampant: vaccination campaigns are a cover for the implantation of microchips used to track people, the vaccine will make you sick, and pharmaceutical companies developed the coronavirus to profit from vaccine development and sales.[14] Driven by these conspiracy theories, some clinicians destroyed the vaccine to "protect the public," while other individuals staged several attempts to disrupt vaccine production.

A conspiracy theory about the dangers of 5G technology resurfaced in 2023, morphing from a claim that 5G exposure makes the human body more susceptible to coronavirus infection to a claim that 5G exposure leads to sterility. Nationwide, more than 50 instances of arson or other damage to wireless towers and telecom equipment have been recorded.[15]

In 2024, a conspiracy theory about fluoride in drinking water re-emerged, fueled by viral videos of a "credible" scientist and doctor demonstrating a link between fluoride and lower scores on intelligence quotient (IQ) tests. Concerned citizens organized rallies in numerous localities to demand a halt to water fluorination, while politicians called for hearings to investigate the safety of adding fluoride to the water supply. Several water treatment plants reported break-ins and the destruction of sensitive monitoring equipment, and dams received credible threats.

Considerations

What initiatives are necessary to account for security risks and vulnerabilities that could arise from social disruptions due to the unchecked spread of conspiracy theories?

- *What plausible steps can the federal government take to address the spread of disinformation that could lead to a threat to critical infrastructure? How might CISA specifically contribute?*
- *How could CISA and federal agencies better support critical infrastructure owners in their efforts to maintain trust with the public?*
- *How can you support critical infrastructure partners in becoming more informed about vulnerabilities that could arise from a breakdown in trust and social cohesion?*

---

[14] Davey Alba and Sheera Frenkel, "From Voter Fraud to Vaccine Lies: Misinformation Peddlers Shift Gears," *New York Times*, Dec. 16, 2020, https://www.nytimes.com/2020/12/16/technology/from-voter-fraud-to-vaccine-lies-misinformation-peddlers-shift-gears.html.
[15] Adam Satariano and Davey Alba, "Burning Cell Towers, Out of Baseless Fear They Spread the Virus," *New York Times*, Apr. 10, 2020, https://www.nytimes.com/2020/04/10/technology/coronavirus-5g-uk.html.

APPENDIX II: TECHNOLOGICAL DISRUPTOR

RACIAL BIASES FROM FACIAL RECOGNITION APPLICATIONS FUEL CIVIL UNREST

In 2024, public confidence in the police remains near the all-time lows recorded during the rallies and protests in the summer of 2020.[16] A popular documentary series premieres on a video streaming site, igniting a firestorm of interest in the use of facial recognition technology. The docuseries centers around the case of Violet Thomas, an African American woman on death row whose arrest and conviction for a murder was largely predicated on identification via facial recognition software used by law enforcement. The docuseries makes the case that the convicted woman is an unlikely suspect and would not have even been on law enforcement's radar had it not been for the use of facial recognition, which is known to be less accurate when identifying men and women of color. Additional episodes demonstrate how biases in facial recognition applications disadvantage men and women of color in security screenings at international ports of entry, airports, and other transit hubs and shed light on racial biases linked to broader artificial intelligence (AI) applications that support employment and promotion decisions, loan approvals, and even medical diagnoses.[17]

The popularity of the docuseries leads to a public outcry, including a recurring rally at the prison housing Violet Thomas, civil disobedience against the use of facial recognition (including staged sit-ins to disrupt court cases in which protestors wear costumes that intentionally disrupt facial recognition systems and demonstrations outside companies that develop facial recognition technologies), and advocacy efforts to pressure officials into changing policies regarding facial recognition. Activists demand the cessation of law enforcement use of facial recognition technologies, as well as reviews of other cases in which identification via facial recognition was used as evidence. In some cities, clashes between protesters and law enforcement lead to the destruction of property. One online campaign calls for citizens to damage traffic and other public and private surveillance cameras, which have become ubiquitous nationwide.

Considerations

As facial recognition and other AI applications become more prevalent, what initiatives could mitigate current concerns about racial biases?

- *How can facial recognition and other AI applications be used safely and ethically in society?*
- *Given that many of the elements of facial recognition and other AI applications are proprietary, what recourse should be available to individuals who feel that they may have faced discrimination in instances when these applications have been deployed?*
- *How could CISA and federal agencies better support and ensure ethical uses of facial recognition and other AI applications?*

---

[16] Aimee Ortiz, "Confidence in Police Is at Record Low, Gallup Survey Finds," *New York Times*, Aug. 12, 2020, https://www.nytimes.com/2020/08/12/us/gallup-poll-police.html; and Jeffrey M. Jones, "Black, White Adults' Confidence Diverges Most on Police," Aug. 12, 2020, https://news.gallup.com/poll/317114/black-white-adults-confidence-diverges-police.aspx.
[17] William Crumpler, "The Problem of Bias in Facial Recognition," Center for Strategic & International Studies, May 1, 2020, https://www.csis.org/blogs/technology-policy-blog/problem-bias-facial-recognition; and Alex Najibi, "Racial Discrimination in Face Recognition Technology," Oct. 24, 2020, http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

APPENDIX III: ECONOMIC DISRUPTOR

POST-PANDEMIC ECONOMIC SLUMP FUELS DISCONTENT AND LOSS OF TRUST IN GOVERNMENT

In the years following the COVID-19 pandemic, an economic depression stubbornly persists in many parts of the country. In 2022, Congress passes another stimulus package intended to jumpstart the economy. A significant portion of the stimulus funds are for businesses to invest in new infrastructure and automation, as well as workforce training initiatives for those who remain out of work. However, the workers who lost their jobs because of automation tend to forgo government-sponsored retraining,[18] and many of the workforce retraining initiatives falter. Unflattering social media coverage has only exacerbated the situation, labeling retraining events as "re-education centers" and drawing comparisons to Chinese work camps.

Social media fringe groups, in particular, take advantage of the widening wealth gap and ballooning federal debt to propagate a false narrative that politicians in Washington, DC, have "sold us out," which has fueled resentment and calls for action against government institutions.[19] By 2025, several fringe groups have become increasingly radical, having gone as far as staging a series of coordinated attacks on federal offices in Detroit, Pittsburgh, Cincinnati, Milwaukee, and Chicago.

Considerations

What initiatives are necessary to account for security risks and vulnerabilities that could arise as a result of economic disparities?

- *What plausible steps can the federal government take to address the spread of disinformation that could present physical risks to critical infrastructures associated with civil unrest and risks to the financial system and governance structures? How might CISA specifically contribute?*
- *How could CISA and federal agencies better support critical infrastructure owners in their efforts to maintain trust with the public?*
- *How could you support critical infrastructure partners in becoming more informed about potential versus arising threats from a breakdown in trust and social cohesion?*
- *How should you support critical infrastructure partners' efforts to achieve the right balance between economic growth/automation and workforce realignment?*
- *How could CISA and federal agencies better support critical infrastructure owners in their efforts to implement workforce retraining initiatives?*
- *How could critical infrastructure owners mitigate concerns and possible backlash—both internal and external to their organizations—from implementing automation?*

---

[18] Ljubica Nedelkoska and Glenda Quintini, "Automation, Skills Use and Training," *OECD,* Working Papers No. 202, Mar. 8, 2018, http://dx.doi.org/10.1787/2e2f4eea-en.

[19] Rens Willems, "When Do Inequalities Cause Conflict? – Focus on Citizenship and Property Rights," Nov. 21, 2012, https://www.thebrokeronline.eu/when-do-inequalities-cause-conflict/; Megan Sheets, "How the Pandemic Made America's Richest Even Richer," Jan. 18, 2021, https://mol.im/a/9160417; Michael Massing, "Most Political Unrest Has One Big Root Cause: Soaring Inequality," *Guardian*, Jan. 24, 2020, https://www.theguardian.com/commentisfree/2020/jan/24/most-political-unrest-has-one-big-root-cause-soaring-inequality; and Catherine Kress, "The Economics of Social Unrest," Mar. 10, 2020, https://www.blackrock.com/americas-offshore/en/insights/the-economics-of-social-unrest.

APPENDIX V: POLITICAL DISRUPTOR

DEEPFAKE VIDEOS THREATEN ELECTION INTEGRITY

AI-enabled digital manipulation tools have simplified the development of realistic fake videos and audios—so called "deepfakes." These tools—such as FakeApp, which was used in 2018 to develop a deepfake video of former President Barack Obama—are readily available for download on mobile phones, making it free and relatively easy to produce convincing face swaps.[20] Experts warned about the possibility of malicious deepfake videos influencing past elections, but there was no evidence of it occurring widely.

That all changed during the 2024 election cycle. With media attention focused on the Presidential election and high-profile Senate races, several down ballot and local elections across the U.S. were derailed by deepfake videos.[21] In a disconcerting trend, most of the deepfake videos targeted female candidates, superimposing their faces on pornographic images.

Additionally, shortly after a U.S. Representative Election Day victory, a video surfaced showing him using racist language while being secretly videotaped at a private fundraising event. Numerous petitions immediately surfaced on social media calling for the Representative to resign, and his opponent called for his expulsion from Congress. Although the Representative admitted to giving a speech at the event, he denied using racist language and claimed his voice was mimicked on the video.

As the 2026 primary season approaches, polls show an overwhelming concern among the public about the legitimacy of elections if they don't know the "truth" about the candidates, but they also reveal the public is more willing to accept whatever "truth" paints their preferred candidate in a more favorable light. Candidates from across the political spectrum all agree that the use of fake videos as a campaign tool is a significant threat to the integrity of elections and promise not to use them. However, recognizing the success of deepfakes in influencing the 2024 election, many candidates do not actively discourage their supporters from using such tactics.

Considerations

What initiatives can you think of to safeguard the integrity of elections?

- *What plausible steps can the federal government take to address the spread of deepfakes that could present a threat to free and fair elections? How might CISA specifically contribute?*
- *How could CISA and federal agencies mitigate the erosion of public trust in the results of elections?*
- *How should critical infrastructure owners and operators prepare for a future in which their reputations could come under attack from deepfake videos?*

---

[20] Kevin Roose, "Here Come the Fake Videos, Too," *New York Times*, Mar. 4, 2018, https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html.
[21] Tim Mak and Dina Temple-Raston, "Where Are the Deepfakes in this Presidential Election?" NPR, Oct. 1, 2020, https://www.npr.org/2020/10/01/918223033/where-are-the-deepfakes-in-this-presidential-election.

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