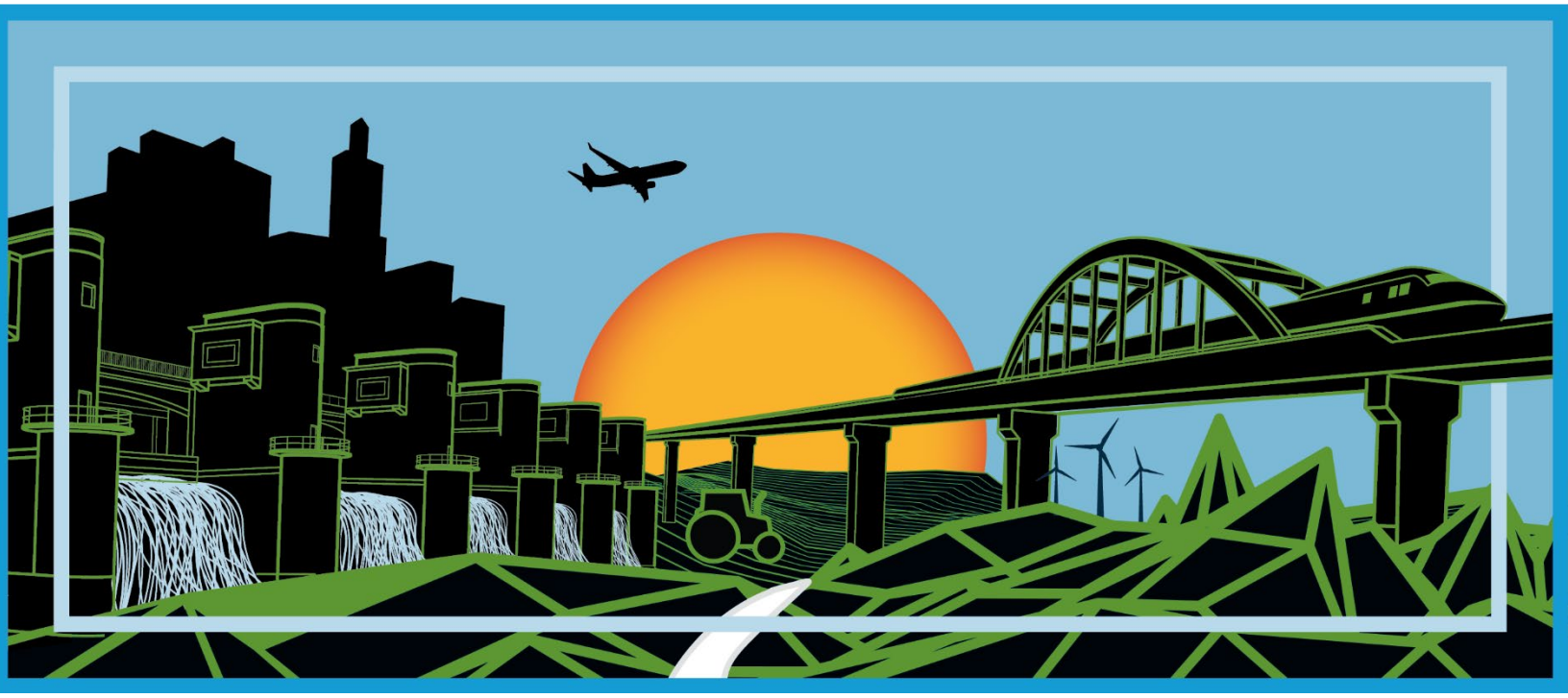

Secure Tomorrow Series

Alternative Futures: Quantum Technologies Controller Guide

Publication: August 2021
Cybersecurity and Infrastructure Security Agency

WELCOME AND INTRODUCTIONS

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

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

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

The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center (NRMC) has developed this game to assist stakeholders across the critical infrastructure community to self-facilitate and conduct foresight activities that will enable them to derive actionable insights about the future, identify emerging risks, and proactively develop corresponding risk management strategies to implement now. One goal of the Secure Tomorrow Series is to develop a repeatable and defensible process that (1) identifies emerging and evolving risks to critical infrastructure systems, and (2) identifies and analyzes the key indicators, trends, accelerators, and derailers associated with those risks to help critical infrastructure stakeholders direct their risk management activities.

As such, today you will be playing as yourselves, bringing your knowledge, experience, and perspectives to debate strategies that will shape critical infrastructure resilience and security in light of potential advancements in quantum 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 to 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 critical infrastructure owners increase the security and resilience of their systems in preparation of future issues that could arise from progress in and use of quantum technologies. 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 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, 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 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/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 example 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 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

For the purposes of this game, we define quantum technologies as those technologies associated with understanding and manipulating quantum phenomena (such as entanglement and superposition)[1] for acquiring, communicating, and processing information. Although this encompasses technologies such as quantum sensors and quantum networks, the scenarios addressed in this game focus on quantum computing. Players are encouraged, however, to consider and comment on potential ramifications that could spill over into other quantum technologies during their deliberations.

Quantum computing is an emerging technology. General-purpose quantum computers currently do not exist and are not expected in the near-term future. A variety of quantum platforms are actively being explored (e.g., ion traps, superconducting circuits), with numerous unknowns to address and technological advancements to achieve before quantum computing's promise can be realized. The term "noisy intermediate-scale quantum" (NISQ) was coined to describe the current era of quantum computing, which is characterized by devices with 50 to a few hundred quantum bits (qubits)[2] that are imperfectly controlled (i.e., noisy). Although researchers hope to find useful applications even with quantum computers in the NISQ era, millions of physical qubits may be necessary to achieve a general-purpose quantum computer.

Once realized, though, such computers are thought to present significant opportunities and risks because of their advantage over classical computers for solving certain types of problems.

- *Quantum simulation has the potential to inform and significantly improve the design of pharmaceuticals, catalysts, and materials.*

---

[1] *Entanglement* is defined as a property in which two or more quantum objects in a system can be intrinsically linked, allowing measurement of one object to dictate the possible measurement outcomes for the others without regard to the distance among them. *Superposition* is defined as the ability of quantum systems to exist in two or more states simultaneously. Congressional Research Service. In Focus Report, Defense Primer: Quantum Technology. June 7, 2021. See: https://crsreports.congress.gov/product/pdf/IF/IF11836/2

[2] "A qubit is a computing unit that leverages the principle of superposition to encode information." Congressional Research Service. *In Focus Report, Defense Primer: Quantum Technology.* June 7, 2021.
See: https://crsreports.congress.gov/product/pdf/IF/IF11836/2

- *Shor's algorithm, an efficient quantum algorithm for factoring large numbers, threatens to break public key encryption, which is central to the security of digital certificates and is used to secure communications and transactions over the internet.*

Opinions vary among experts as to when quantum computers will be sufficiently powerful for these applications. Nevertheless, cryptographic concerns are prompting the development of post-quantum cryptographic algorithms and other approaches that would be safe from the threat of quantum computing. Additionally, large technology firms and venture capitalists are making substantial investments based on quantum computing's potential. In 2021 alone, an estimate of more than $1.7 billion of private funding was announced for quantum computing start-ups. The current levels of excitement and investment surrounding quantum computing relative to its maturity have led to concerns about excessive hype.

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 pertaining to quantum technologies. These scenarios may limit player actions, reflect new capabilities achieved through quantum technologies, or require players to consider the implications of an event. [Identify the first player to log on by name.] *As the first player to log on, you can choose which STEEP category you would like to explore for Round 1.* [See Appendices I–V. Please note that each disruptor ends with a question that should be announced to the group after reading through the disruptor narrative, to clarify the issue that players will be addressing for the disruptor. Additional discussion questions are included in each appendix to serve as prompts or as questions for open discussion periods.]

LET'S PLAY

Round 1

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

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

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

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

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

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

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

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

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

The Cybersecurity and Infrastructure Security Agency (CISA) has produced these scenarios to initiate and facilitate discussion. The situations described here are hypothetical and speculative and should not be considered the position of the U.S. Government. All names, characters, organizations, and incidents portrayed in these scenarios are fictitious.

APPENDIX I: SOCIAL DISRUPTOR

PRIVACY AND PUBLIC PERCEPTION OF QUANTUM COMPUTING

For years (decades even), futurists have warned that the development of quantum computing technologies will enable public key encryption (PKE) to be broken, putting at risk all applications that depend on digital information communication technologies. But, up until recently, most individuals and government officials assumed the day when a quantum computer is first able to crack PKE—known as Q Day—would be sufficiently far in the future that all necessary mitigations would be developed and deployed before it arrived.

It has become increasingly evident, however, that Q-Day is approaching much faster than expected and that its impact on privacy may be worse—or even much worse—than originally believed. Notably, in 2024, Softprocess announced a major breakthrough in building a working quantum computer that solved problems previously unsolvable using other methods. Other breakthroughs soon followed, such as when the technology company, NMBIS, far surpassed its own quantum roadmap of building a more powerful quantum computer system in 2026.

The first (initially classified) reports of quantum-enabled unauthorized access into legacy systems started permeating into public consciousness less than a year later, before the news program "360 Degrees" aired its troubling exposé in 2028. Almost overnight, people grew existentially anxious about what this all meant for them personally, questioning the ability to keep secret anything they do, and calling into question the integrity of web browsing, online purchasing, using mobile phones and email, safeguarding financial and medical records, and (after realizing that quantum decryption can be applied retrospectively) the security of effectively all existing data.

What initiatives and policies can you think of to mitigate the effects of a growing public fear of an impending loss of privacy?

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.]

- *Might concerns be assuaged by introducing new quantum-era encryption/decryption regulations, or regulatory protections of stored data? What form would such regulations take (e.g., constraining the length of time data are allowed to "sit on the shelf")?*
- *What can critical infrastructure owners and operators do to become better informed about vulnerabilities to data centers and potential risks to the data housed there?*
- *How can CISA and the U.S. Federal Government better communicate the potential dangers and possible mitigations of the loss of individual privacy and the integrity of personal data?*

- *Progress in quantum sensors may lead to related privacy fears of intrusion into individuals' personal space, with ever more capable sensors that might see behind walls or read "brain states." How might these concerns be mitigated?*

APPENDIX II: TECHNOLOGICAL DISRUPTOR

LETHARGIC INDUSTRIAL SECTORS HIT BY A CYBERATTACK

Projected timelines for the appearance of a cryptographically relevant quantum computer (CRQC) that can break PKE have varied widely. Federal agencies have been developing mitigation measures, including quantum key distribution, quantum random number generators, and post-quantum cryptographic (PQC) algorithms,[3] but the time available to implement necessary countermeasures has been highly uncertain.

Weak links within the "network-of-networks" of critical infrastructure will be those elements that have failed to closely monitor developments in quantum computing and quantum-resistant encryption; failed to inventory legacy and cryptographically compromised legacy systems; failed to develop plans to re-encrypt data-at-rest (and to re-sign any digitally signed artifacts); or sluggishly followed national guidance for PQC migration.

Two cyberattacks in 2035, following announcements of successfully developed CRQCs, highlighted the ramifications of not acting quickly enough to mitigate the quantum threat:

- *Criminal hackers orchestrated a coordinated nationwide cyberattack on the software and hardware of Mexlar's new generation of completely autonomous cars, targeting both sensors (e.g., causing them to malfunction), and performance (e.g., using CRQCs to break into a manufacturer's over-the-air software updates to inject a malicious code).*
- *Several U.S. smart cities go into virtual "meltdown" as CRQCs are used to: (1) endanger public health by manipulating the functions of water treatment plants and distribution systems, (2) create dangerous driving conditions by corrupting real-time data in intelligent transportation systems, and (3) induce power outages by generating critical fluctuations in energy price data in automated demand-response systems.*

What initiatives can you think of to enable critical infrastructure stakeholders to recognize both the severity of the quantum threat and the importance of developing a post-quantum strategy in a timely manner?

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 can be done to support and encourage efforts to take pre-emptive mitigating actions sooner (e.g., cataloging all extant cryptography practices and protocols; creating a list of who "owns" software maintenance and delivery updates; identifying "weak link" legacy algorithms, data formats, and application programming interfaces of cryptographic libraries)?*

[3] The most notable PQC effort is led by the National Institute of Standards and Technology (NIST), which—though draft standards are expected by 2024—possibly entails a much longer process. NIST is expected to announce an additional round of evaluating PQC algorithm candidates between now and 2028, which will take 18 to 24 months to complete, and after which a second phase will be run, reopening the competition to new signature algorithms (and requires at least another two rounds). Reference: "Post-Quantum Cryptography," https://csrc.nist.gov/projects/post-quantum-cryptography.

- *What steps should be taken to encourage stakeholders to keep up with general developments in quantum computing and quantum-resistant encryption, and to follow relevant national guidance on post-quantum migration?*

APPENDIX III: ECONOMIC DISRUPTOR

CRYPTOASSET MARKET CRASH

In 2035, officials have determined—much to their surprise—that one or more foreign adversaries have likely reached a level of quantum computing capability, such that a significant percentage of cryptoassets in circulation are vulnerable to attack. For example, federal agencies have identified cases in which the digital signatures used to sign for cryptocurrency transactions have been broken, resulting in illicit transfers and liquidation of various cryptoassets. With the realization that cryptoassets are vulnerable to attack, owners are scrambling to liquidate their holdings or move them over to a quantum-resistant digital signature scheme. But these attempts have come too little, too late as cryptoasset markets have collapsed because of vulnerability fears.

The widespread failure of smart services in the city of Silvershoe may have provided the initial hints that led federal agencies to discover the digital signature vulnerability. Five years ago, Silvershoe officials turned to blockchain technologies in an effort to make their city "smarter" and reduce budget costs. Beginning in June 2030, residents of Silvershoe experienced anomalous charges for city services, data integrity issues with various contracts, and even a temporary breakdown in traffic signaling that snarled downtown traffic for hours. Although initially attributed to cyberattacks, these incidents all appear to have stemmed from cracked encryption-coded signing keys and forged digital signatures.

What initiatives can you think of to avoid disruptions to the economy that might arise from sufficiently powerful quantum computers?

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 steps should be taken to better prepare cryptoasset owners for the post-quantum cryptography era?*
- *What are the economic and security implications associated with the emergence of smart cities and e-government services and the potential vulnerabilities of relying on blockchain technology? What are potential mitigating actions?*

APPENDIX IV: ENVIRONMENTAL DISRUPTOR

ENVIRONMENTAL MIRACLE

Yesterday, Wogpol announced not one, but two breakthroughs in catalyst development: one that can operate at much lower temperatures and pressures than the current Haber-Bosch process for producing ammonia fertilizer; and another that enables more efficient conversion of water into hydrogen.

Numerous scientists hailed the announcements as game changers for combating climate change and the breakthrough in quantum computing performance that has been sought for decades. Others grumbled about the secrecy that preceded these developments. For years now, Wogpol has been silent about its progress for developing quantum computers and has increasingly focused on bringing talent in key application areas in house, rather than relying on partnerships. As a result, the full potential of the scientific community has not been leveraged. While these developments breathe new life into the prospects of a hydrogen economy, some lawmakers expressed similar dismay that the surprise announcement has prevented officials from guiding expectations appropriately and has led to lost time in preparing the infrastructure needed to support green hydrogen's use.

The two new catalysts promise to be the first of many potential advances in materials and pharmaceuticals prompted by quantum simulation. But even as Wogpol stock is at an all-time high, security experts have expressed concerns about one company controlling a tool with so many applications—including the realization of cryptography concerns and the ability to control the direction of research for at least the next few years.

What initiatives can you think of to speed up the realization and spread of these environmental opportunities while safeguarding the underlying technologies enabling them?

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 are the potential security implications of this capability being monopolized by one company?*
- *How should federal agencies approach communication and coordination with the private sector as quantum computing capabilities are nearing fruition?*
- *What steps should be taken to increase agility and prepare for infrastructure changes that might arise from quantum simulations?*

APPENDIX V: POLITICAL DISRUPTOR

QUANTUM WINTER

While many believed that cryptographically relevant quantum computers were inevitable, there were also those who believed a "quantum winter" was just as likely.[4] *With the benefit of hindsight indicating loss of funding and talent looking for other opportunities, it is now apparent that the nay-sayers were right all along.*

In the 2020s, even as researchers continued developing new ways of building qubits and quantum circuits and engaged in heated debates about the merits of various qubit mediums, quantum computing itself showed little progress. The best quantum computers were still far too noisy and unable to sustain coherent states for long enough to come close to cracking any codes. Meanwhile, algorithm development was similarly stymied. There have been no new "breakthrough" algorithms that are able to run exponentially faster on quantum computers than on their classical counterparts. The last "success" was back in 2024, when a quantum computer was finally able to factor a "large" 21-digit number. While this exceeded the record at the time by 7 digits, this achievement was a ridiculously small number next to the 617 decimal digits needed to crack a 2,048-bit public key. Who could have predicted that this "record" would still be standing 10 years later? After much early excitement, the increasingly lethargic progress and lack of any short-term applications have led officials to question continued federal investment in quantum computing, touting several examples of failed companies that received significant federal funding.

What initiatives can you think of for policy- and decision-makers to consider that will prepare for a future in which today's enormous investment in developing quantum technologies is judged to have led to unacceptably diminishing returns?

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 metrics should be used to assess technological progress and "return on investment"?*
- *How might the various interrelated quantum technologies (computers, sensing, and communications) be disentangled or insulated in the event that only one technology (say, quantum computers) succumbs to a winter?*
- *What steps can be taken to avoid a quantum winter and to ensure agility and resiliency when coming out of one?*
- *In the event of a quantum winter, what are the decision mechanisms by which funds will be reallocated?*

[4] "Quantum winter" is defined as a state in which the development of quantum computing technologies loses momentum because of a lack of short-term applications or slow progress.

APPENDIX VI: GAME SCHEDULE

TABLE 1—SCHEDULE FOR CONDUCTING THE MATRIX GAME

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