Secure Tomorrow Series:

Quantum Technologies Player Guide

Publication: August 2023
Cybersecurity and Infrastructure Security Agency

Background

How prepared are critical infrastructure sectors in light of potential advancements in quantum technologies? *Alternative Futures: Quantum Technologies* presents you with scenarios that could plausibly occur within the next 10 to 15 years. During each round, you and your opponents will take turns proposing initiatives and debating strategies that will shape critical infrastructure resilience and security in light of potential advancements in quantum technologies. How successfully you manage to present your arguments for (or against) these initiatives determine their chances of success. Depending on your role for the round, you can score points for either successfully implementing or countering initiatives.

The Cybersecurity and Infrastructure Security Agency (CISA) National Risk Management Center 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.

For players, the game hopefully represents a fun and interactive way for you to think broadly about future threats and opportunities, learn from your peers, and identify strategies to inform preparedness activities.

The game takes about three hours to complete. This includes an introduction and description of the current state, three rounds of gameplay (each about 45 minutes long), and a final 20-minute open-discussion period to collect any final feedback from players and wrap up the game.

Player Roles and Assignments

At the start of the game, each player will be assigned one of three roles. Players will rotate roles in subsequent rounds, so that they fill different roles through the course of the game. The three roles are as follows:

- The Innovator(s): Responsible for developing initiatives and arguments in support of those initiatives.
- The Devil's Advocate: Responsible for developing counterarguments to the initiatives proposed by the Innovator.
- The Judge: Responsible for adjudicating the validity of the Innovator's arguments versus the counterarguments made by the Devil's Advocate for a particular initiative and determining the initiative's likelihood of success.

Players will bring their personal knowledge, experience, and perspectives to debate strategies that will shape critical infrastructure resilience and security in light of potential advancements in quantum technologies. Players should consider policies, programs, investments, public-private partnerships, research and development, or other actions that, if successfully put into motion today, they believe will better position and prepare one or more critical infrastructure sectors for the future. In preparing for the game, players may want to think about the following questions:

- What risks and opportunities are associated with the advancement of quantum technologies?
- What are the implications for future critical infrastructure resilience and security?
- Are there specific ramifications for one or more critical infrastructure sectors?
- Is there a role for CISA to address threats and uncertainties associated with the advancement of quantum technologies?
- Are there other trends that may influence the advancement of quantum technologies?

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 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.
- 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.

Playing the Game

Alternative Futures: Quantum Technologies has three rounds, each of which will present the players with a scenario that could plausibly occur within the next 10 to 15 years. In Round 1, the Innovator(s) will have 15 minutes to identify up to three initiatives that will support critical infrastructure resilience and security in response to the specified scenario disruptor. For each initiative, the Innovator(s) will then describe up to three supporting arguments for why the initiative will succeed.

The Devil's Advocate will then have 10 minutes to describe up to three counterarguments for each initiative. Each counterargument can be directed at one or more of the arguments presented in favor of the initiative's success or underscore a new concern that may cause the initiative to fail. The Innovator(s) will then have 5 minutes to rebut any or all of the counterarguments. The Judge will listen to both sides of the debate and ultimately determine if each initiative has a high, medium, or low likelihood of success. The Judge will have 5 minutes to present the rationale for his or her determinations and roll a 20-sided die to see if each initiative succeeds or fails.

The die simulates the unpredictability of the supporting environment for initiatives, and the game's inability to account for all positive and negative factors that might influence success.

- An initiative with a **high** likelihood of success will be implemented with a roll of 6 or higher (75 percent chance).
- An initiative with a **medium** likelihood of success will be implemented with a roll of 11 or higher (50 percent chance).
- An initiative with a **low** likelihood of success will be implemented with a roll of 16 or higher (25 percent chance).

An open-discussion period may occur after resolving the success or failure of the initiatives to continue any discussions cut short by previous time constraints.

In Rounds 2 and 3, the participants will rotate roles.

Disruptors

Social, technological, environmental, economic, and political (STEEP) influences have the potential to alter the trajectory of future trends or disrupt them altogether. For example: urbanization is a social disruptor that has the potential to significantly affect the resilience of lifeline sectors; an election outcome is a potential political disruptor that could affect funding for critical infrastructure projects; cyberattacks are a technological disruptor with a wide range of cascading implications for all critical infrastructure sectors.

To account for a changing future environment, each round features a STEEP disruptor scenario that may limit player actions, alter the trajectory of current trends in the advancement of quantum technologies, or require players to consider the implications of an event. The possible scenarios to choose from during the game are described in Appendices I–V. As an added incentive for players to craft compelling arguments and counterarguments, the winning player of each round is awarded the ability to select the STEEP disruptor category for the next round.

Winning the Game

If the Innovator(s) successfully implement(s) a majority of the initiatives, the Innovator(s) win(s) the round. Alternatively, if the Devil's Advocate counters a majority of the initiatives, he or she wins the round. While the game is designed to encourage competition between the players, its main purpose is to generate discussions that develop well-conceived and thought-provoking initiatives. Your collective subject matter expertise is what matters, regardless of the outcomes of each round.

Game Schedule

TABLE 1—SCHEDULE FOR CONDUCTING THE MATRIX GAME

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

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

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

APPENDIX I: SOCIAL DISRUPTOR

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?

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,[1] 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?

[1] 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 require at least another two rounds. Reference: "Post-Quantum Cryptography," https://csrc.nist.gov/projects/post-quantum-cryptography.

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?

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?

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.[2] 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?

[2] "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.