SCENARIOS WORKSHOP FACILITATOR(S) GUIDE

Secure Tomorrow Series

***Non-federal facilitators**: The Cybersecurity and Infrastructure Security Agency (CISA) has provided this toolkit as a starting point for your organization to address these critical issues. Please feel free to expand upon or adapt these exercises and tools to your needs. In several places throughout the document, we have provided guidance for federal facilitators regarding participants, process, and information protections. This guidance is based upon federal requirements, which may differ from state and local considerations. Please consult with your organization to consider what language or actions you will need to take in hosting a workshop session.*

GOAL

This workshop uses scenario narratives to help participants explore ways in which the operating environment for critical infrastructure owners and operators may evolve over the next 5–10 years, and how this evolution may affect the security and resilience of critical infrastructure systems. In particular, the workshop's four scenarios center on plausible future changes pertaining to the topics of (1) data storage and transmission, (2) anonymity and privacy, and (3) trust and social cohesion.

Workshop participants will leave the workshop having identified a prioritized set of risk mitigation strategies that will increase critical infrastructure resilience and security, regardless of future uncertainties.

KEY WORKSHOP OUTPUTS

- Identification of significant issues and questions—to address now and in the future—for the various strategic operating environments posed in each of the four scenarios
- A prioritized set of risk mitigation strategies that would increase security and resilience in most, if not all, of the four scenarios

BACKGROUND

In the context of this workshop, a scenario is a story with plausible cause and effect linkages that connect a future condition with the present while illustrating key decisions, events, and consequences throughout the narrative. By using a small set of carefully crafted scenarios, organizations can avoid focusing on just a single future (i.e., *the* future) and develop strategies and plans that are viable over a range of possible futures. This is the underlying premise behind the scenarios workshop sessions.

RECOMMENDED PARTICIPANTS

*[**Please note:** Invitations to participate should focus on mid-to-senior career-level individuals who are interested in exploring longer-term risks to critical infrastructure to enable effective risk mitigation. To provoke new lines of thinking about risks to critical infrastructure systems (either directly or through cascading impacts), we recommend that you seek broad representation from regional Cybersecurity and Infrastructure Security Agency (CISA) personnel; state, local, tribal, and territorial planners; fusion center and intelligence community representatives; and other private-sector, non-profit, think-tank, and academic stakeholders. In particular, individuals with interest and expertise in data storage and transmission, privacy and anonymity, and trust and social cohesion, and individuals who are already familiar with strategic foresight, are encouraged to participate. Because the workshop divides participants into four groups, please consider how you will achieve mixing and balancing different perspectives and expertise.]*

[Once known, this section of the guide would list the workshop participants, their titles, and the agencies/organizations they represent. If permitted by the workshop sponsor, the facilitator should consider providing participant biographical information to all participants ahead of the workshop]

WORKSHOP FORMAT

The workshop activities were designed to occur over eight hours, either as a virtual event over two consecutive afternoons or as a one-day, in-person event. The remainder of this guide is built around a virtual execution of the workshop, which would use a virtual meeting platform.

FACILITATION STAFF

- One lead facilitator/workshop coordinator
- Three scenario facilitators
- Four documentation leads

Note: Each facilitator is responsible for one scenario. The lead facilitator also serves as a scenario facilitator.

SUPPORT MATERIALS

- STS Scenarios Workshop: Introduction and Roadmap Slides
- STS Scenarios Workshop: Are We There Yet Participant Poll
- STS Scenarios Workshop: Are We There Yet Results Slides

WORKSHOP PREPARATION

Hosting a virtual scenarios workshop is a major undertaking and can be considered a capstone activity that follows execution of matrix games or cross-impacts sessions. For additional details about the steps necessary to plan a virtual workshop, please see Appendix A: Workshop Planning Considerations.

Facilitators should review in detail the support materials that pertain to their assigned scenario. Although they should focus most of their attention on their assigned scenario, facilitators should also review the remaining scenarios.

Prior to the workshop, the workshop coordinator will assign participants (maximizing diversity of backgrounds in each group) to one of four groups. Each group will focus on one of the scenario

narratives. Participants should receive their assigned scenario narrative at least one week before the workshop as a read ahead. Facilitators should review their list of assigned participants and familiarize themselves with the background and affiliation of each participant.

The lead facilitator/workshop coordinator should plan to hold at least one orientation meeting that requires attendance from all scenario facilitators and documentation leads. During this meeting, the lead facilitator/workshop coordinator should walk through the workshop agenda and sessions, allowing sufficient time for facilitation staff to ask questions about the workshop itself and detailed questions about the scenarios.

AGENDA

DAY ONE	
1:00–1:45pm	Framing the workshop: welcome, participant introductions, workshop objectives, and event roadmap (*plenary session*)
1:45–2:30pm	Icebreaker exercise: Are we there yet? (*plenary session*)
2:30–2:45pm	Break
2:45–4:45pm	Scenario breakouts ▪ Participant introductions ▪ Scenario familiarization and build out ▪ Identification of emerging and evolving risks and associated needs ▪ Risk mitigation strategies
4:45–4:55pm	Closing remarks (*plenary session*)

DAY TWO	
1:00–1:10pm	Welcome back and roadmap for the day's activities (*plenary session*)
1:10–1:55pm	Alternative future stress test: Round 1
1:55–2:40pm	Alternative future stress test: Round 2
2:40–2:55pm	Break
2:55–3:40pm	Alternative future stress test: Round 3
3:40–4:30pm	Synthesis and reflection (*plenary session*)
4:30–4:45pm	Closing remarks (*plenary session*)

GENERAL INSTRUCTIONS

- **Foster and maintain a collaborative and respectful atmosphere.** Encourage different observations, opinions, and perspectives. The discussions will explore a variety of policies, actions, and issues, and participants will likely display different degrees of expertise on discussion topics. The breakouts are no-fault, not-for-attribution sessions focusing on the identification, analysis, and generation of solutions for upcoming issues of concern.
- **Encourage participants to speak from their perspective.** There may be strategic needs that are prominent for particular stakeholder groups. A participant's unique perspective can be used as a starting point for broadening the discussion as to how it might apply to other stakeholder groups. If a participant is speaking from the perspective of a particular stakeholder group, ask other stakeholder groups about how this might also apply to them
- **Anchor participants in the scenarios.** Ask participants to refer to content from the scenario narrative whenever possible to make the discussion more concrete.
- **Reinforce the future context of discussions.** Include references to the time period when presenting materials and emphasize, when appropriate, the scenario time horizon of 5–10 years in discussions to prevent participants from lapsing into present-day concerns.
- **Focus on critical infrastructure security and resilience.** Keep the group on topic. How does whatever is being discussed lead to a connection to risk for critical infrastructure security and resilience? It can be connected indirectly, and facilitators can prompt discussion about any complexities and tradeoffs involved, but they should always return to critical infrastructure security and resilience. In other words, as the group is identifying emerging or evolving threats, also have group members elaborate on the nexus to critical infrastructure, if it is not obvious.

FRAMING THE WORKSHOP

DAY ONE: 1:00–1:45 PM	
Description	The workshop coordinator provides a brief introduction and welcome to all participants and introduces the lead facilitator (if necessary). The lead facilitator then explains the goal for the workshop and walks participants through how the various sessions will integrate to achieve this goal.
Session Objectives	State the goal of the workshop and discuss how the sessions in the workshop agenda fit together to achieve this goal
Outputs	Improved participant understanding of the workshop
Duration	45 minutes
Supporting Materials	STS Scenarios Workshop: Introduction and Roadmap Slides
Staffing Requirements	▪ Workshop coordinator ▪ Lead facilitator ▪ Senior leader representing the hosting organization
Breakdown	1. Welcome (workshop coordinator) 2. Thank you to participants (senior leader representing host organization) 3. Review of workshop objectives and desired outputs (lead facilitator) 4. Roadmap of workshop sessions (lead facilitator)
Facilitator Talking Points	Please work from the provided PowerPoint slides
Additional Notes	None

ICEBREAKER EXERCISE: ARE WE THERE YET?

DAY ONE: 1:45–2:30 PM	
Description	The lead facilitator will conduct an icebreaker exercise with participants. The exercise involves presenting participants with a series of eight topic areas (e.g., space travel, autonomous vehicles). Participants will be polled on their perspectives about how far society will have progressed a decade from now in each area. The facilitator will ask participants to select from a list of pre-established answers.
Session Objectives	▪ Orient participants' thinking toward the longer-term future ▪ Allow participants to see how their views about the future compare with those of others ▪ Familiarize participants with the concept of underlying drivers of change by exploring participants' rationale for their answer selections
Outputs	None
Duration	45 minutes
Supporting Materials	▪ STS Scenarios Workshop: Are We There Yet Participant Poll ▪ STS Scenarios Workshop: Are We There Yet Results Slides
Staffing Requirements	Lead facilitator
Breakdown	1. Relay exercise instructions (lead facilitator) 2. Walk through each of the eight topic areas, then facilitate discussion of the polling results (lead facilitator)
Facilitator Guidance	▪ Initial talking points: ○ Thinking about the future in longer-term timeframes can be difficult, so we didn't want to shock you by throwing you straightaway into deliberations about different states of the world 5–10 years from now. In this session, we're going to try and orient your thinking toward a longer-term time horizon. ○ This session is fairly short. Think of it as an icebreaker to the workshop and a chance for participants to stretch their thinking forward in time in order to see how their views of the future compare with other participants. *At this point, transition to using the STS Scenarios Workshop Are We There Yet Results Slides.* ▪ Three slides address each topic in the slide deck (please refer to the slide deck). The first slide simply contains images that quickly describe the topic to participants. The second slide lists the specific polling question with associated progress milestones as answer options. These milestones are topic specific and listed in order of increasing progress. The third slide presents the polling results. After showing the polling results, ask volunteers to provide their perspectives. Call attention to interesting features of the

	answer distribution (e.g., extremes, most popular, explanations for bimodal distributions).
Additional Notes	▪ Some virtual platforms can execute live polling. If live polling is used, facilitators should work to pre-populate the polling questions (as listed in the polling question sheet) ahead of the workshop. Facilitators should also remember to delete the second and third slides associated with each of the eight topics in the slide template. ▪ If you will not be obtaining polling results live during this activity, please coordinate with the workshop coordinator to ensure that participants receive the polling worksheet (STS Scenarios Workshop: Are We There Yet Participant Poll) ahead of the workshop, and that their responses have been returned, tabulated, and inserted into the slide template ahead of time. ▪ If you are unable to perform live polling or send out the polling worksheet ahead of time, you may use the existing charts shown in the STS Scenarios Workshop: Are We There Yet Results Slides. The results in this deck are from an execution of this exercise held at CISA headquarters with a diverse group of representatives from government agencies, think tanks, academia, and private-sector companies. Please note, however, that the time horizon for this execution of Are We There Yet? was slightly longer (to the year 2035).

SCENARIO BREAKOUTS

DAY ONE: 2:45–4:45 PM	
Description	Participants will break into four separate groups, each exploring an alternative future scenario. The facilitator assigned to the group will lead a discussion about the scenario, fleshing out elements of this future based on participant interests and subject matter expertise. Participants will identify and then prioritize a set of risk mitigation strategies that would better prepare critical infrastructure stakeholders for any emerging or evolving risks (and opportunities) that may exist in this future scenario.
Session Objectives	▪ To engage participants with their scenario—i.e., to create ties between components of the narrative and their particular backgrounds (e.g., industry, knowledge, experiences, perspectives) ▪ To understand how scenario conditions shape strategic needs and associated risk mitigation strategies necessary to address these needs ▪ To prioritize and identify a maximum of five risk mitigation strategies based on what was written or extrapolated from the scenario narrative. These will feed into sessions on Day Two that stress-test these risk mitigation strategies against alternative future scenarios
Outputs	A prioritized list of up to five recommended risk mitigation strategies to improve critical infrastructure resilience and security in the world described by the scenario
Duration	2 hours
Supporting Materials	Scenario narratives: ▪ STS Scenarios Workshop: Life Under a Microscope ▪ STS Scenarios Workshop: A Fragmented World ▪ STS Scenarios Workshop: Deep Disinformation ▪ STS Scenarios Workshop: A New Wave of Cooperation
Staffing Requirements	▪ Four facilitators (one for each scenario) ▪ Four documentation leads (one for each scenario)
Breakdown	Begin by assisting participants in discussing and fleshing out the scenario. During this discussion, you should encourage participants to identify ramifications associated with the various changes, trends, or events captured in the narrative; emerging and evolving risks (and opportunities); and other important drivers or concerns related to key elements of the scenario narrative (that were not captured). After immersing participants in their scenario, the facilitator will assist participants in identifying and then prioritizing a set of five risk mitigation strategies to address critical needs (to enhance critical infrastructure resilience and security) arising from the scenario. Participants will discuss these risk mitigation strategies in the workshop's subsequent "stress-testing" sessions. These strategies should be prepared in slide presentation format for use in the stress-testing sessions.

	Key steps during the session include the following: 1. Conduct participant introductions. 2. Allocate 10 minutes for participants to read through the scenario. 3. Assist the group with working through the scenario and highlight points of interest and how they tie potentially to concerns for critical infrastructure resilience and security. For example, you may want to ask each participant—as they read through the scenario—to prepare answers to the following questions: o Name an element of the scenario that resonated with you—i.e., what did you find most interesting or compelling? o What is an emerging or evolving risk discussed or hinted at—either related to your previous answer or to another part of the scenario—that you are most concerned about? o What are the ramifications (direct or indirect) of this emerging and evolving risk for critical infrastructure security and resilience? o What is a risk mitigation strategy that you might employ to address this risk? If discussions stall, you may want to reference concerns and discussion points flagged in your scenario's Detailed Scenario Breakdown. When relevant, please remind participants to tie their statements to the scenario write-up, so individuals can skim the narrative for context. 4. Roughly one hour and fifteen minutes into the session, if any major issues of interest built into the scenario narrative have not been addressed, introduce them for group discussion. Please note that the facilitator, workshop coordinator, and other relevant workshop stakeholders should decide ahead of time which issues the facilitator should try to cover during the session, using the Detailed Scenario Breakdown as a starting point for such determinations. 5. If the group identifies more than five risk mitigation strategies, they will need to prioritize five of them to present during the "stress-test" sessions. Please allow sufficient time for prioritization. You may wish to insert a short break for participants; during the break, you can refine the participant inputs and develop a strawman list of the top risk mitigation strategies. Allocate at least 15 minutes after the break for participants to react to the strawman, select the top-five risk mitigation strategies, and further refine the risk mitigation strategy statements.
Facilitator Guidance	▪ State the desired output from this session. At the end of this session, we would like to identify a prioritized set of five risk mitigation strategies. ▪ Re-emphasize that the scenario narratives are meant to provide just enough structure and content for a productive discussion. A three- to five-page narrative cannot fully describe a future state of the world, especially if the goal is to make the scenarios easy to read. We wanted to take advantage of the group's enormous collective expertise to flesh out those parts of the narrative that are most pertinent to critical infrastructure security and resilience. ▪ Bend, do not break, the scenario. If places exist where the narrative did not probe deeply enough, or where a portion of the narrative was intriguing but

did not get a lot of space, we encourage participants to fill in these gaps or make refinements (as long as you feel the discussion is heading in a probative direction). However, 180 degree shifts from the proposed scenario that are not permitted.

- Focus on critical infrastructure security and resilience. How does whatever is being said connect to critical infrastructure security and resilience? It can be indirectly connected, and we can certainly have a discussion about any complexities and tradeoffs involved, but we always want to come back to critical infrastructure security and resilience.
- Encourage participants to speak from their perspectives. Strategic needs may exist for particular critical infrastructure stakeholder groups and communities. We can use this as a starting point for broadening the discussion to other critical infrastructure stakeholder groups.
- Engage participants with the scenario. If a participant feels disconnected from the group, ask what resonated most for him or her. Was there a concern that was not explicitly addressed, but would have ramifications for his or her organization, industry, or mission? How might the risks mentioned translate to his or her circumstances?
- Return them to the scenario. Does the narrative already provide examples and evidence that a strategic need exists? Please also refer to the scenario as a means of making the discussion more concrete.
- Foreshadow the other scenarios, as relevant. Doing so should help participants orient to the upcoming stress-test sessions on Day Two.
- Outline what will happen during the stress test rounds. The ultimate output of the workshop is a set of risk mitigation strategies that are robust against a multiplicity of futures. Thus, group members will be presenting their risk mitigation strategies to other scenario groups to discuss the relevance and efficacy of these strategies under different future operating environments. Participants need to have a firm understanding of the large role they will play in communicating the risk mitigation strategies to their peers on Day Two.

Facilitator Prompting Questions

For additional questions specific to content within the narrative, please refer to the appropriate scenario.

Questions to assist with fleshing out and familiarizing participants with this future reality:

- What portions of the scenario resonated most with you?
- What emerging and evolving risks were discussed or hinted at in this scenario that you are most concerned about?
- What are the ramifications of these emerging and evolving risks for critical infrastructure security and resilience (if not obvious)?
- How might some of the issues, trends, and threats identified in the scenario affect your particular organization/industry (ask as appropriate)?

Questions to assist with identifying risk mitigation strategies:

- What strategic needs or capabilities must be addressed by critical infrastructure stakeholders as a result of the threats, as well as the prevailing conditions, that you have identified for this scenario?

	▪ What risk mitigation strategies might you propose to address these needs or develop these capabilities? ▪ Which risks do you feel the nation is currently least prepared to address? What risk mitigation strategies would you propose to address these risks? ▪ What would we wish to have done currently to be positioned better to address these challenges in the next 5–10 years? ▪ How might critical infrastructure stakeholder roles and missions need to change and evolve to address the threats of concern? ▪ Are changes to existing authorities, resources, and understanding necessary? Questions to assist with prioritization of risk mitigation strategies: ▪ Why would this be among your top five strategies? ▪ Are any of the risk mitigation strategies that you have identified too generic or implausible to implement? ▪ Does this risk mitigation strategy represent a radical departure from the status quo? Are current activities occurring within the critical infrastructure stakeholder community likely to address the underlying strategic need that this strategy is meant to address? ▪ Are there any risk mitigation strategies that would help address multiple threats or strategic needs associated with the scenario?
Additional Notes	Before the workshop, the workshop coordinator assigns participants (maximizing diversity of backgrounds in each group) into one of four groups. Each group will focus on one of the scenario narratives, and all participants should receive their assigned scenario narrative at least one week in advance of the workshop as a read ahead.

STRESS-TEST ROUNDS

DAY TWO: 1:10–3:40 PM	
Description	The facilitator for each scenario group will divide the participant group in half. One half will rotate to another scenario group and present its risk mitigation strategies to that receiving group. The scenario group members receiving this presentation will assess the relevance and utility of implementing these risk mitigation strategies under the different operating environment and circumstances of their own scenario, engaging in discussions with the presenting group. Three rounds of stress tests will occur; by the end of these rounds, participants will have had their risk mitigation strategies assessed for robustness against the other workshop scenarios.
Session Objectives	To discuss and perform a basic assessment of how relevant the presenting group's risk mitigation strategies are for the receiving group's scenario.
Outputs	▪ Notes on which risk mitigation strategies were judged to be more relevant and useful to alternative futures. ▪ Notes on possible modifications to risk mitigation strategies that would make them more relevant and useful to alternative futures.
Duration	2.5 hours
Supporting Materials	▪ Facilitators should be prepared to share a slide on the virtual meeting platform with the risk mitigation strategies of each visiting group. ▪ Scenario synopses one-pager ("Secure Tomorrow Series_Scenario Synopses.docx").
Staffing Requirements	▪ Four facilitators (one for each scenario). ▪ Four documentation leads (one for each scenario).
Breakdown	1. Divide the group into two teams. One team will rotate to present the group's risk mitigation strategies. The other team will listen to another group's presentation of risk mitigation strategies and discuss the relevance of these strategies to this alternative scenario. Each round will run for 45 minutes. You can simply rotate in order of the scenario numbers. For example, Scenario 3 presenters will go to the Scenario 4 breakout during Round 1, and then on to the Scenario 1 breakout in Round 2, and finally to the Scenario 2 breakout in Round 3. Alternate which team will present the group's risk mitigation strategies for each stress-test round. 2. During each round, both the visiting group and the audience group should begin by presenting brief report outs on their scenarios. Presenters should feel free to refer to the summary of their scenario in the scenario synopses one-pager (Secure Tomorrow Series Scenarios Workshop Synopses). 3. The visiting group will then go through its risk mitigation strategies one by one. The facilitator should share a slide on the virtual meeting platform with the risk mitigation strategies of the visiting group. 4. For each risk mitigation strategy, the two groups will engage in a facilitated discussion about how well the risk mitigation strategy fits the alternative

	scenario and what modifications might improve the strategy's alignment to the scenario (if not initially a good fit). 5. Facilitators lead participants to conduct a final vote of the relevance of the risk mitigation strategy to the alternative scenario (e.g., not a fit, a partial fit, or an excellent fit).
Facilitator Guidance	▪ Balance the two teams in each group. Use your best judgment to balance the strengths of both teams based on their insights and participation. For example, avoid assigning all of your most active participants to the away team, as the home team will then be less capable of engaging with the groups in an active discussion about the relevance of their risk mitigation strategies. ▪ Re-emphasize the purpose of stress-testing. Before sending half of the group to another breakout room for the first round of stress testing, facilitators should reiterate the purpose of the three stress-test rounds. Day Two focuses on stress testing the risk mitigation strategies identified for the primary scenario against the other scenarios. A key concept in scenario-based planning is using multiple future scenarios to identify strategies that are robust against uncertainty. The underlying rationale is that because we cannot successfully predict the future, we should treat the future as a set of plausible alternatives against which our strategic planning efforts need to be robust. The three stress-test rounds are one way of executing this concept in practice.
Facilitator Prompting Questions	▪ If implemented, would this risk mitigation strategy be effective in your scenario? What concerns might you have about implementing this strategy? ▪ How would this risk mitigation strategy rank relative to the ones you identified for your scenario? ▪ Are there conditions in this alternative future that would make this strategy more difficult or easier to implement? ▪ How could you modify the existing risk mitigation strategy statement so that it is more relevant to your scenario, without destroying the intent of the team that originated it?
Additional Notes	None

SYNTHESIS AND REFLECTION

DAY TWO: 3:40–4:30 PM	
Description	In this plenary session, the lead facilitator asks participants to provide their perspectives on what they learned from the three rounds of stress testing and solicits overall reactions to the concerns and ideas presented during the workshop.
Session Objectives	To provide an opportunity for participants to reflect more broadly on what they learned from the Stress-Test Rounds and the overall workshop
Outputs	▪ Additional insight and detail on risk mitigation strategies ▪ A feeling of closure for participants, increasing their willingness to support future efforts
Duration	50 minutes
Supporting Materials	▪ None
Staffing Requirements	▪ Lead facilitator ▪ Senior leader representing the hosting organization ▪ Documentation lead
Breakdown	▪ Solicitation of remarks by scenario group (lead facilitator) ▪ Solicitation of final remarks or reactions to anything discussed at the workshop (lead facilitator)
Facilitator Prompting Questions	▪ What were your key takeaways from the workshop? ▪ Did you learn of any risk mitigation strategies from other scenario groups that surprised you or that you would like to comment on?
Additional Notes	If relevant, the lead facilitator may want to relay information about any products that will be generated from the workshop (e.g., a report) during this session.

SCENARIO OVERVIEW

TABLE 1. SCENARIO OVERVIEW AND COMPARISON

No.	Title	Risks			Disruptive Incident(s)
		Data Transmission and Storage	Privacy and Anonymity	Social Cohesion and Trust	
1	Life Under a Microscope	Transmission speed increased, storage less secure	Decreased	—	SARS-19 pandemic, proliferation of Internet of Things (IoT), micro-targeting of critical infrastructure personnel
2	A Fragmented World	Global transmission fragile and fragmented, Storage more secure	Varies between countries	—	SARS-19 pandemic, critical cyberattack, segmentation of global internet
3	Deep Disinformation	—	Decreased due to pervasive online data gathering	Decreased due to lack of trust and increasing partisanship	Growing influence of deepfakes, terror attack
4	A New Wave of Cooperation	Transmission speed increased, storage more secure	Increased	Improved	Series of nation state cyberattacks, passage of major legislation, Iranian gray zone operations

SCENARIO #1: LIFE UNDER A MICROSCOPE

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

BRIEF DESCRIPTION

Because of advances in wireless technology, transmission of data now occurs at unprecedented rates. Data security, however, has not kept pace. The rapid movement of mass amounts of data in a poorly secured environment results in a digital world that is a cybercriminal's playground with, unsurprisingly, increased cyber incidents. Despite general concerns about the loss of personal information in the U.S., the true scope and scale of data theft and data breaches are unclear because of a technical inability to maintain data provenance (and therefore identify and attribute cyberattacks). While discussions on changes to online tracking and privacy protection authorities are ongoing, legislative approaches are unlikely to provide a practical solution in the current environment. The security implications of this situation are soon realized four years from now, when a third-party data broker is implicated in the release of sensitive information with cyber and physical security effects.

SCENARIO CONTEXT

- Set up as congressional testimony provided in the aftermath of a series of cyber and physical attacks on personnel working at a nuclear power plant. The narrative ties these attacks to foreign adversary use of third-party data brokers. The testimony underscores the challenges of providing protections for sensitive data in an increasingly connected world.
- Outlines several trends facilitating increased collection of personal data, such as growing reliance on data broker services, the proliferation of IoT devices, and decreasing public concern about online and personal privacy.
- Explores various ways in which the SARS-19 pandemic is accelerating change.
- Examines potential concerns related to growing reliance on cloud-based infrastructure.

FACILITATION QUESTIONS – TAILORED

Please note: Broader, more general facilitation questions—common to all four scenarios—are located in the Scenario Breakouts section of this facilitator's guide. Additional discussion points, as tied to specific potions of the scenario narrative, are listed in each scenario's "Detailed Scenario Breakdown."

- What are the implications of an operating environment in which you see transition to cloud-based services and potential adoption of IoT and edge devices into your organization's operations?
    - How might this influence your concerns about cybersecurity moving forward?
- How might individual attitudes toward data privacy affect data security? What other ramifications might exist?
- How might the types and extent of disruption to critical infrastructure functions and services change as reliance on IoT devices, edge devices, and cloud-based services grows? Are there sector-specific concerns that warrant greater attention?

- What other concerns could you see evolving from the ability to micro-target individuals?
- With the growing reliance on and increased availability of information from third-party data brokers, what are the implications for government's role in their oversight? How might public expectations and perceptions of the government's role in cybersecurity oversight change?
- How might the nature of cyberattacks change (e.g., targets, types of attack, frequency, actors), and what operational challenges would these changes create?

On "Cyber and Physical Attacks on Atomica Nuclear Power Plant Personnel"
A Hearing Before the
Senate Homeland Security and Governmental Affairs Committee
and
U.S. Senate Committee on Energy and Natural Resources
Written Testimony Submitted by FBI Cyber Division Director Jonathan Style

September 18, 2026

Chairman, Chairwoman, Ranking Members, and members of the Committees, thank you for the opportunity to testify before you today regarding the Federal Bureau of Investigation's (FBI) and our federal partners' efforts to understand, mitigate, and respond to the recent cyber and physical attacks on personnel from the Atomica nuclear power plant. [1] We take these recent attacks with the utmost seriousness. The initial response of the U.S. government was swift and measured; however, we must do more to ensure that critical infrastructure operators are protected and that we are not vulnerable to such attacks in the future. Part of doing more is understanding the history and environment that has led to such attacks, while also assessing and mitigating against future risks.

Incident Assessment

Between November 2025 and May 2026, a series of cyber and physical attacks, some successful, were executed against a number of security and key operational personnel from the Atomica nuclear power plant. The attacks were highly targeted to those individuals, as demonstrated by the fact that the attackers had privileged, private, and sensitive information on the individuals' identities, locations, and personal habits. [2]

Since the first attacks, FBI, other components of the Department of Justice (DOJ), and the Department of Homeland Security Cybersecurity and Infrastructure Security Agency have worked together closely to identify and neutralize the source of these attacks. The FBI's Cyber Division is responsible for investigating, dismantling, and prosecuting cybercrimes. Through our efforts, many of the perpetrators have been identified, pursued, and arrested.

Initially, we faced challenges in our ability to identify the sources of personal and sensitive information that enabled these attacks. It was not until June 12, 2026, that information obtained by a major news outlet provided us with the break that we were searching for. The media source implicated a third-party data broker, SecurePI, in the sale of sensitive data on Atomica personnel to a foreign corporation with close ties to Russia. [3] For those unaware, SecurePI has been helping Atomica revamp its personnel security and has been assisting the company in managing the sensitive information collected during security and background investigations.

We have been able to attribute the breach of sensitive data to an insider who worked at SecurePI. [4] This individual had access to the information necessary to review and grant access control and security privileges. The individual responsible for the breach was paid to produce analytical products for Russia to allow micro-targeting of individuals. [5] The data sold also included packets of data that were de-anonymized to allow Russia to amass a great deal of information on these individuals and their families. [6]

DOJ and our partner agencies have taken swift action against that individual and against the Russian government.

Factors Contributing to the Attacks

Although an insider clearly enabled these attacks, other factors, many dating back more than a decade, have contributed to the possibility of this type of breach to occur. The prevalence of third-party data brokers is one such contributing factor.

Third-party data brokers generate, for profit, consumer profiles by piecing together information from a variety of disparate and unrelated sources. [7] It is now faster and cheaper, not to mention more thorough, to conduct a search with one of these brokers than to go through almost any public sector process. By 2023, standard practice was to engage these services to run background checks on people rather than to use police departments. The popularity of these services has skyrocketed and they are used regularly around the country to vet job applicants, prospective tenants, childcare workers, potential loan recipients, and others in need of identity verification.

Make no mistake, these companies collect potentially sensitive information about individuals such as financial fitness, employment history, political affiliations, webpages frequently visited, close social connections, and categorization into social groups for all manner of applications. Our society has become increasingly reliant on these companies in order to function. Today, local, state, and federal government agencies in the U.S. are developing processes to integrate a pseudo social-credit system—leveraging a variety of social and civic behavioral indicators along with financial indicators—through the use of third-party data brokers. [8] Local law enforcement departments nationwide are using these systems to support investigations, which have enhanced safety and policing and improved public relations. For security reasons, the U.S. government has limited its use of third-party data brokers to those that are owned and operated in the U.S. Ironically, the adoption of third-party data brokers was driven at least in part to help address insider threats and help organizations better assess job applicants and monitor employees. Unfortunately, as we have seen, these services are not without their own risks.

Another contributing factor is simply the amount of data that third-party data brokers (and other organizations) have on individuals, including critical infrastructure owners and operators. The largest data brokers have amassed thousands of data points on billions of individuals worldwide. [9] The individuals who executed the attacks leveraged personal information on Atomica personnel, including location-tracking data and personal habits, to target their cyber and physical activities. Over the past decade, the proliferation and collection of this type of personal data corresponded to the proliferation of connected personal digital/virtual assistants (often referred to as Internet of Things, or IoT, devices), along with a decrease in society's concern about online and personal privacy. [10]

Many attribute these changes in connectedness and the decrease in privacy to a post–SARS-19 world. [11] As the U.S. (and the world) recovered from SARS-19 and rebounded from the concurrent economic impacts, concerns about online privacy seemed to dwindle. [12] In the late 2010s, we saw increasing concern over individuals' cybersecurity and privacy, as exemplified by the European Union's General Data Protection Regulation (GDPR) legislation. But by 2023, the tides seemed to have turned. Little privacy legislation was enacted in the post–SARS-19 period. There was also little public dissent to online tracking, as the benefits of enabled devices seemed to outweigh any hypothetical costs. [13] Without privacy legislation, the rise in IoT-enabled and connected devices corresponded with a decrease in real-world privacy. Individuals these days expect little privacy when their real-world movements and online activities are continuously tracked.

Before proceeding, I would like to note that my intention today is not to make a case against IoT-enabled devices but, rather, to highlight the complex nature of enabling digital connectivity while maintaining privacy and security. In the post–SARS-19 era, IoT devices, coupled with rapid data transmission enabled by 5G networks, have been employed with great benefit to the U.S. and other nations. [14] For example:

- Health-status tracking apps (deployed on personal devices) enabled the rapid collection and dissemination of contact tracing and SARS-19 vaccination and immunity data tracking. Despite initial resistance, pandemic fatigue and the desire for a "return to normal" made the majority of those in the U.S. eventually assent to this collection and dissemination of data.
- The SARS-19 pandemic also led to an increase in remote work, which many employees and companies sought to continue, at least in part, after the pandemic. [15] As more employees and companies turned to telework and as more people grew accustomed to a virtual world, the market for IoT-enabled devices that would help them work at home (e.g., mixed reality and augmented reality devices, automated system monitoring and control devices, predictive maintenance devices) boomed.
- The SARS-19 pandemic also demonstrated weaknesses in the U.S. supply chain for some critical supplies and resources (e.g., food, paper products, and medical supplies). In addition to increasing U.S. manufacturing capabilities in these areas to secure the supply chain, real-time IoT- and 5G-enabled tracking gave suppliers a much clearer picture and control of critical supplies, including the ability to rapidly assess and reroute shipments to areas of need.
- Beginning in 2020, deployment of 5G increased internet access to many rural areas, achieving more than 70 percent penetration in the U.S. by the end of 2025.

As these benefits were realized, the proliferation of IoT and advanced wireless technologies continued, leading to parallel growth in data collected on individuals and an increase in sensitive data collected and stored by organizations.

Future Threat Assessment

Looking forward, the risks—both cyber and physical—presented by the proliferation of sensitive data collection and the limitations of privacy protections will persist. Additional factors exist that can contribute to the feasibility and criticality of cyber and physical attacks on organizations and individuals. Specifically, a lack of security standards for cloud infrastructure and IoT devices presents considerable challenges to securing cyberspace, [16] a topic on which I have testified previously.

To provide you with a bit of background, an increasing number of companies started taking advantage of cloud services, continuing a trend that began prior to the 2020s, especially as the amount of data these companies needed to store increased and the cost of cloud services decreased. Since 2020, the amount of sensitive data stored in the cloud has increased exponentially. [17] Additionally, cloud users can access a variety of cloud services, including both cloud and hybrid architectures. However, as organizations began to implement multi-cloud infrastructures, many lacked—and continue to lack—a thorough understanding of their entire cloud footprint. Many do not appreciate that cloud security is a shared responsibility between the provider and users. [18] A lack of cloud IT security professionals also contributes to the number of poorly secured cloud infrastructures. [19]

Meanwhile, IoT devices often lack appropriate security. Some attempts have been made to secure IoT infrastructure, such as the 2020 IoT Cybersecurity Improvement Act. Unfortunately, that act and others that followed have done little to improve the nation's overall IoT security because they have failed to sway a sufficient number of manufacturers into adopting the prescribed standards. Although market forces have encouraged IoT device security, the rapid expansion in the number of IoT devices and the lack of security requirements have still resulted in many poorly secured networked devices. [20]

Poorly secured cloud infrastructures and IoT devices present a multitude of easy access points for sensitive data and systems. [21] Although this attack on Atomica personnel was the result of an insider threat, in the current environment an insider is not required to gain access to sensitive data in many cases.

To help manage and attempt to secure sensitive and personal data, many organizations are leveraging data Security as a Service (SECaaS) and Disaster Recovery as a Service (DRaaS); however, this is not enough. The rapid expansion of IoT devices, rapid data transmission rates, instances of insecure IoT devices and cloud services, and the data available on individuals and organizations has put the U.S. in a vulnerable position. This vulnerability is exemplified by the fact that over the past few years there has been a dramatic increase (500 percent since 2022) in the number of successful cyberattacks.

With rapid data transmission rates, nefarious actors are able to exfiltrate massive amounts of data in a very short amount of time. They need only very brief access to a system to steal terabytes and even petabytes of data, making automatic network defenses less effective. The rollout of many insecure IoT devices in the manufacturing sector has led to vulnerabilities from industrial espionage in critical supply chains. [22] Unfortunately, the ability to move large amounts of data rapidly and the rapid expansion of cloud users and services has also made movement of data, and thus data provenance, harder to track. [23]

Understanding and identifying these risks is not the principal challenge we face. Rather, our principal challenge is determining how we can reverse course in some areas and take actions that support and provide the benefits of our connected world, but provide protections for sensitive personal, private sector, and government data. [24] To counter the threats we face, the U.S. government must collaborate with the private sector to secure IoT devices, secure personal information, secure cloud infrastructures, and monitor insider threats better. [25]

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

DETAILED SCENARIO BREAKDOWN: LIFE UNDER A MICROSCOPE

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
1	12	…the recent cyber and physical attacks on personnel from the Atomica nuclear power plant.	**NOTE:** Scenario 2 and Scenario 4 also cover a major cyberattack, however Scenario 2 focuses more on the financial impacts and geopolitical implications, while Scenario 4 discusses its physical impacts and geopolitical implications, as well as cyber espionage.
2	22	The attacks were highly targeted to those individuals, as demonstrated by the fact that the attackers had privileged, private, and sensitive information on the individuals' identities, locations, and personal habits.	**CONCERN**: Micro-targeting of key individuals for cyber and physical attacks. **INFO**: ▪ Detailed location data on individual daily movements is for sale to companies that seek insights into consumer habits and behavior, often without consumer knowledge and/or consent. ▪ In August 2020, an NSA guidance warned of the threat that third-party access to location data can pose to national security, with hackers able to cross-reference the app's location by looking at Wi-Fi signals or to location data in photos.
3	32	The media source implicated a third-party data broker, SecurePI, in the sale of sensitive data on Atomica personnel to a foreign corporation with close ties to Russia.	**CONCERN:** Foreign adversary intelligence collection through third-party data brokers. **NOTE**: In this narrative, an insider threat is responsible for the sale of sensitive data. More broadly, however, a data broker can effectively sell, analyze, or manipulate data without any restrictions once the broker receives the data. Foreign adversaries can presumably take advantage of the unregulated data-broker industry. Vermont is the only state with a law in place regulating data brokers. This statute is limited in scope and does not grant Vermonters any new rights, such as the ability to opt-out of data collection or bring legal action against law breakers.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
4	35	We have been able to attribute the breach of sensitive data to an insider who worked at SecurePI.	**CONCERN:** Insider threat. **DP**: ▪ What could the amassing and consolidation of data mean for insider threats? ▪ What are the long-term ramifications of the SARS-19 pandemic on the workplace and how does this affect the risk of insider threats?
5	38	The individual responsible for the breach was paid to produce analytical products for Russia to allow micro-targeting of individuals.	**NOTE:** Scenario 3 also covers micro-targeting of individuals based on collected data, however, as a means to spread disinformation. **INFO:** Unrestricted access to aggregated datasets can tempt employees into data abuse or theft. In November 2019, DOJ charged two former Twitter employees with using their access to collect private user information on Twitter users who were critical of the Saudi government.
6	40	The data sold also included packets of data that were de-anonymized to allow Russia to amass a great deal of information on these individuals and their families.	**CONCERN:** Data aggregation and the "mosaic effect." The "mosaic effect" of data aggregation occurs when information from an isolated dataset does not pose a risk (e.g., of identifying an individual), but could pose such a risk when combined with other available information. **INFO:** Although organizations strip datasets of PII, with advances in machine learning, artificial intelligence, and supercomputers, numerous cases have shown that users can be re-identified. For example, Rocher et al. found that 99.98 percent of Americans would be correctly re-identified in any dataset using 15 demographic attributes (*Nature Communications*, July 2019).
7	48	Third-party data brokers generate, for profit, consumer profiles by piecing together information from a variety of disparate and unrelated sources.	**INFO:** ▪ In the absence of a comprehensive U.S. data privacy law, virtually no constraints exist on the types and amount of user data organizations can collect, keep, or process. ▪ Online tracking and targeted advertising erode user privacy by following users across platforms. With a growing consumer digital footprint, data from third-party cookies, location services, "fingerprinting," pre-built user profiles, etc. allow interested parties to micro-target users and tailor disinformation campaigns. **DP**: What issues should a comprehensive U.S. data privacy law address?

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
8	60	Our society has become increasingly reliant on these companies in order to function. Today, local, state, and federal government agencies in the U.S. are developing processes to integrate a pseudo social-credit system—leveraging a variety of social and civic behavioral indicators along with financial indicators—through the use of third-party data brokers.	**INFO**: China is currently developing and implementing a social-credit system, which incorporates financial, social, and civic indicators and is meant monitor, assess, and shape the behavior of its citizens and businesses. While China's implementation of a government run system is unique, the use of aggregated data to assess trustworthiness is familiar to Americans in the forms of credit scores, user ratings on apps, and other social rankings. **DP**: If U.S. society trends in this direction, what are the ramifications for personal privacy? What are potential lessons-learned from China's current efforts?
9	68	Another contributing factor is simply the amount of data that third-party data brokers (and other organizations) have on individuals, including critical infrastructure owners and operators. The largest data brokers have amassed thousands of data points on billions of individuals worldwide.	**INFO:** For example, Oracle claims to have data on 80 percent of the U.S.'s internet-using population, with over 30,000 data attributes per user.
10	73	Over the past decade, the proliferation and collection of this type of personal data corresponded to the proliferation of connected personal digital/virtual assistants (often referred to as internet of things, or IoT, devices), along with a decrease in society's concern about online and personal privacy.	**NOTE:** Scenario 3 also explores the impacts of a continued negative privacy trend. **INFO**: The IoT is a system of sensors, actuators, and devices connected through networks (and the internet) to enable communication and integration. The IoT can link appliances, home security systems, utilities, wearable devices, infrastructure systems, personal and commercial vehicles, and many other systems, equipment, and assets to enhance operations, maintenance, and customer experiences. Experts estimated that 20 to 47 billion devices will be in the IoT by 2020. By 2030, experts predict the number of connected IoT devices to increase to 125 billion. With this increase, more opportunities will exist for malicious actors to launch cyberattacks against and from network-connected devices. The 2016 DEF CON, for example, exposed 47 vulnerabilities affecting 23 IoT-enabled systems from 21 manufacturers. Furthermore, the interconnected nature of the IoT means that once in one system, shortcuts may be found to others. For example, a relatively benign (and less secure) system or device, such as a smart thermostat, may provide access to a critical system, such as a power plant.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
11	75	Many attribute these changes in connectedness and the decrease in privacy to a post–SARS-19 world.	**DP:** What other societal impacts from the pandemic may emerge or continue, and how might they affect critical infrastructure system resilience and security?
12	76	As the U.S. (and the world) recovered from SARS-19 and rebounded from the concurrent economic impacts, concerns about online privacy seemed to dwindle.	**DP**: What types of privacy legislation might have been enacted to prevent this scenario from coming to pass? What would be the major components of such legislation?
13	80	There was also little public dissent to online tracking, as the benefits of enabled devices seemed to outweigh any hypothetical costs.	**INFO**: According to a 2019 Pew Research Center survey, even though 81 percent of Americans say the potential risks outweigh the benefits when it comes to companies collecting data, 63 percent do not think it is possible to go through daily life without sharing their data.
14	87	In the post–SARS-19 era, IoT devices, coupled with rapid data transmission enabled by 5G networks, have been employed with great benefit to the U.S. and other nations.	**NOTE:** Scenario 2 and Scenario 4 also discuss the benefits associated with technological enhancements, specifically advances in IoT and 5G, although in Scenario 2, these advances are undercut by other technological issues. **DP:** ▪ Are there other opportunities beyond the ones mentioned in the scenario that you feel warrant discussion? ▪ For brevity and storytelling purposes, the narrative does not include an expansive discussion on 5G or 6G. But what do you see as the major opportunities and vulnerabilities that have arisen from the incorporation of these technologies to support critical infrastructure systems? ▪ Similarly, the narrative does not identify any risks that may have emerged from changes catalyzed by the SARS-19 pandemic. What concerns do you see (e.g., with remote work, telemedicine)?
15	93	The SARS-19 pandemic also led to an increase in remote work, which many employees and companies sought to continue, at least in part, after the pandemic.	**NOTE:** Scenario 4 also explores the impact of a continued remote work trend on technology, however, Scenario 4 covers it from a cybersecurity standpoint. **INFO**: A survey of CFOs by Gartner conducting during the SARS-19 pandemic found that 74 percent of organizations plan to shift some employees to remote work permanently.
16	113	…a lack of security standards for cloud infrastructure and IoT devices presents considerable challenges to securing cyberspace…	**NOTE:** Both Scenario 2 and Scenario 4 also discuss standards and the resultant impact on technology development. Scenario 2 focuses on competition in standards setting between the U.S. and China. Scenario 4 takes an alternate

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
			approach of discussing how voluntary standards adopted by industry may improve certain technologies. **DP:** In the subsequent paragraph, the narrative goes on to describe a variety of concerns with greater reliance on the cloud. Did the write-up overlook any important concerns?
17	117	Since 2020, the amount of sensitive data stored in the cloud has increased exponentially.	**INFO:** According to an International Data Corporation (IDC) estimate, two-thirds of data is currently stored in centralized facilities and on personalized electronics. By 2025, 40 percent of data will be stored in the cloud.
18	121	… as organizations began to implement multi-cloud infrastructures, many lacked—and continue to lack—a thorough understanding of their entire cloud footprint. Many do not appreciate that cloud security is a shared responsibility between the provider and users.	**CONCERN:** Enterprises may over-rely on their cloud-storage providers for data security.
19	122	A lack of cloud IT security professionals also contributes to the number of poorly secured cloud infrastructures.	**INFO**: A 2020 Survey Report of cybersecurity professionals by the Enterprise Strategy Group found that cloud security represented the second most significant skills gap amongst industry professionals (second only to application security).
20	128	Unfortunately, that act and others that followed have done little to improve the nation's overall IoT security because they failed to sway a sufficient number of manufacturers into adopting the prescribed standards. Although market forces have encouraged IoT device security, the rapid expansion in the number of IoT devices and the lack of security requirements still resulted in many poorly secured networked devices.	**NOTE**: The outlook on standards in this scenario contrasts with Scenario 4, which takes a more optimistic outlook on the effectiveness of voluntary and federal efforts.
21	130	Poorly secured cloud infrastructures and IoT devices present a multitude of easy access points for sensitive data and systems.	**CONCERN**: Rapidly expanding attack surface for cyberattack.
22	142	The rollout of many insecure IoT devices in the manufacturing sector has led to vulnerabilities from industrial espionage in critical supply chains.	**CONCERN**: Supply chain disruption and industrial espionage.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
23	143	Unfortunately, the ability to move large amounts of data rapidly and the rapid expansion of cloud users and services has also made movement of data, and thus data provenance, harder to track.	**CONCERN:** Data provenance **INFO**: An organization's inability to track the origins and destinations of data can lead to bad insight if the data is "dirty," possibly resulting in monetary losses or poor decision-making. A 2015 survey-based, data-quality study by Experian estimated that U.S. companies, on average, wasted 27 percent of their revenue due to inaccurate or incomplete customer and prospect data. **DP:** What are the ramifications from a data governance perspective?
24	147	…take actions that support and provide the benefits of our connected world, but provide protections for sensitive personal, private sector, and government data.	**DP:** Do you see this as a trade-off, or are there still opportunities to increase both? If so, what actions would you recommend?
25	149	To counter the threats we face, the U.S. government must collaborate with the private sector to secure IoT devices, secure personal information, secure cloud infrastructures, and monitor insider threats better.	**DP:** ▪ Do you agree that these are the areas in which public-private collaboration would be most beneficial? Are there others? If so, what are they? ▪ Can you begin to outline what shape these collaborations would take and what specific outcomes you would be looking to achieve?

SCENARIO #2: A FRAGMENTED WORLD

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

BRIEF DESCRIPTION

International and domestic policy choices result in an Internet that is less reliable, less resilient, and more prone to errors in the next five years. Geopolitical tensions between the U.S. and China lead to mismatched standards in hardware, limiting the deployment of 5G worldwide. Meanwhile, other countries have, for a variety of reasons, implemented controls over their domestic networks and access to the broader internet. As the internet fragments, transfer speeds decrease, routing errors increase, and the cost of doing business grows, affecting numerous National Critical Functions.

SCENARIO CONTEXT

- Presents a summary of presentations from a global forum on data, this scenario highlights a more fragmented global internet and the resulting consequences.
- Identifies three drivers for growing internet fragmentation—competition in standards setting, loss of trust in the global internet, and growing barriers to cross-border data transfers.
- Presents a world in which China and the U.S. pursue different strategies for communications technology, as catalyzed by the SARS-19 pandemic.
- Traces how fundamental insecurities in the internet's design contributed to a massive cybersecurity incident ("the Great Takedown") that galvanized action by countries to take a more restrictive stance on data governance with varying degrees of internet traffic segmentation.

FACILITATION QUESTIONS – TAILORED

Please note: Broader, more general facilitation questions—common to all four scenarios—are located in the Scenario Breakouts section of this facilitator's guide. Additional discussion points, as tied to specific potions of the scenario narrative, are listed in the scenario's "Detailed Scenario Breakdown."

- What are the implications of decreasing security and reliability in data transfers?
- What critical infrastructure sectors might face the greatest risks to the resilience and security of their systems as a result of an increasingly fractured internet?
- What are the security implications of the different paths that the U.S. and China have pursued when it comes to technological advantage?
- What actions can the U.S. take to help reverse the trends of increasing internet segmentation and cyber sovereignty?
- In addition to interoperability, privacy, and trust, what other drivers are you concerned about in accelerating internet fragmentation?

UN World Data Forum: Building the Global Internet

Meeting in Brief

January 12–16, 2026

UN Department of Economic and Social Affairs

The UN World Data Forum is a global platform for governments, private sector entities, academia, international organizations, and civil society groups to discuss critical topics regarding international digital security and connectivity. The Eighth UN World Data Forum, which took place in New York City, January 12–16, discussed issues affecting the flow of data on the internet, their implications, and potential solutions.

The forum's **keynote speech**—"A Fragmenting Internet"—was delivered by Robert Kapoor, the former chairman of the U.S. Federal Communications Commission. Kapoor commented on the technical obstacles that are increasingly limiting the speed and accuracy of global data transfers, attributing them to byzantine data localization requirements, retrogression of interoperability for mobile technology, and segmentation of several national networks from the global internet.

Fragmentation has exponentially increased the rates of internet service disruptions and transfer errors, especially for cross-border data transfers. [1] For users, this means decreased transfer speeds (for example, emails taking longer to reach their destination), increased routing errors (such as being directed to the wrong website after entering a correct URL in the address bar), and increased hijacking of traffic (allowing hackers to observe online activity and steal information). Furthermore, because of the transnational nature of the internet, users' data can be stored in data centers around the world. Thus, issues that apply to cross-border data transfer can affect even "domestic" industries. [2]

Kapoor outlined some of the ways in which the fractured internet has affected critical industries. Industries that depend on rapid global internet connectivity (financial services, manufacturing, entertainment, etc.), for example, face rising costs and increasing downtime, as well as greater difficulty accessing real-time data. [3] Tracking commodities and shipments across the world has become more difficult. These challenges have also undercut investments in 5G and IoT.

As Kapoor also noted, by separating their networks from the global internet, autocratic rulers have additional power to censor their citizens and prevent the free flow of information. [4] He presented the events that transpired in Eskarheem during July 2024 as a case in point: the ruling party shut down Eskarheem's internet for several days to prevent reports of the government's harsh treatment of protestors from spreading to international media.

Building on Kapoor's keynote, a number of the forum's sessions delved into the underlying reasons for growing internet fragmentation. The following are some critical issues that emerged from discussions.

- **Competition in standards setting between the U.S. and China: [5] overcoming barriers and achieving compromise**. One of the key barriers to progress in standards setting has been the inability of the international community to come to a consensus on whose 5G standards to follow: the U.S.'s or China's. During the forum, panelist Jeff McHale, senior fellow at the Silverman Institution, described standards as critical building blocks for making technology safe and

compatible. Currently, however, China is throwing its weight behind international trade and standards-setting organizations that are more susceptible to its growing political influence and away from independent bodies such as the International Organization for Standardization (ISO). [6] As a result, no standards-setting organization is the clear authority, and global standards and interoperability development is effectively gridlocked.

Nora Atkins, senior fellow at Tamarel Law School's Eugene Chen China Center, discussed recent developments in 5G communications standards setting. She described how both the U.S. and China used post–SARS-19 economic stimulus to invest in communications technology. However, the U.S. targeted Artificial Intelligence (AI) and connectivity (5G, Wifi 6, and rural Wifi access), enabling major advances in automation and IoT. [7] In contrast, China doubled down on its earlier successes in 5G, surveillance technology, and quantum communications. These investments continued to yield dividends for China, as well as the many Belt and Road Initiative countries and African authoritarian regimes that China exported its technology to. [8] The investments also increased the competitiveness of many Chinese companies in global markets.

- **Regaining trust in the global internet: working with internet service providers (ISPs) to address past issues and build in security.** The internet is plagued by a fundamental paradox: how to ensure the security of information housed on the internet while also upholding the ideals of freedom and openness that have long been promoted by Western democracies. According to Louis Joyce, co-founder and president of the Center for an Ethical Internet, despite growing reliance on the internet for the critical functioning of society, liberal Western democracies failed to pay sufficient attention to the internet's well-known insecurities, instead allowing private sector interests to dominate internet governance. [9] In retrospect, Joyce claimed, it was clear that the internet was highly at risk of massive disruption, whether it was an attack on physical infrastructure or a disruption of the internet's routing mechanisms.

  Joyce described how this contributed to The Great Takedown, the cybersecurity event that would spark changes in internet governance around the world, [10] directly contributing to present-day internet fragmentation. For years, China had been hacking the Border Gateway Protocol (BGP) to conduct state-sponsored espionage of all types, including man-in-the-middle attacks and hijacking traffic, rerouting data through government-aligned ISPs in China where they could view and potentially manipulate data. [11] BGP issues take place daily and cause small outages, but usually are not noteworthy. [12] However, in 2022, a botched hack of the BGP, widely attributed to the Chinese government, indiscriminately redirected a large segment of the internet through a government-owned ISP in China for nearly an hour. [13] The hack occurred in the middle of the Western world's workday and triggered internet outages that have since been linked to billions of dollars of lost revenue.

  Joyce concluded with a proposed path forward, including new operating standards that would bake in security as a feature of the internet, as well as a plan to get all U.S. ISPs to collectively adopt more secure operating standards, in the hope that other ISPs worldwide will follow suit. [14]

- **Cross-border data transfers: overcoming data transfer friction between different diverse web services, transmission standards, and hardware to improve internet interoperability.** Since internet fragmentation began in earnest in 2022, the general public has become more aware of how a fragmented internet limits the flow of information. Ordinary data transfers, such as emails and file sharing, take significantly longer. For businesses and governments, delays in data transfer—or incorrectly delivered transfer—can be disastrous.

Mary Sullivan, vice president of Pax Technologia LLC, provided an overview of how the fragmentation unfolded. As a response to the events of The Great Takedown, as well as growing concerns about cybersecurity, several nations instituted measures designed to flex their digital independence: [15]

- The EU implemented protectionist policies to prop up domestic technology supply chains [16]
- India, Japan, and Indonesia passed data localization requirements [17]
- Other nations—including some in the EU along with the UK, Australia, India, Vietnam, Kazakhstan, Indonesia, and Iran—segmented at least some degree of their domestic internet from the global internet.

Sullivan described how segmentation creates barriers where previously there were none. Basically, segmentation can occur in two ways: One way involves a country building its own infrastructure, including servers, transmission lines, and routers. This path is expensive, extreme, and not easily reversed, and so far, only Russia and Iran have taken it. Other nations have instead implemented firewalls that monitor and filter incoming web traffic based on IP addresses and keywords. These nations have also rerouted traffic from some international websites to domestic-based equivalents. Although this may sound innocuous, the outcome is a highly fragmented internet that is slower, less reliable, and less resilient.

Fragmentation has been compounded by the impacts of increasingly severe weather. Storms, heat waves, and sea level rise increasingly threaten the physical infrastructure of the internet, including thousands of cables, data centers, points of presence, landing stations, and internet exchange points. [18] These conditions are increasing service disruptions and forcing providers and companies to rethink their data flows, even as fewer avenues are available to route data through.

Sullivan concluded with a passionate call to action, noting that the path forward involves rethinking the way in which security is designed to restore trust in the global internet.

The **closing presentation** was made by Rong Zhou, head of the Internet Service Providers Conglomerate. Zhou called on the international community to work together to halt the splintering of the internet and expressed optimism that the forum would help address issues around data transfer and storage by creating a consensus on interoperability, privacy, and trust. During the question-and-answer portion of this discussion, a forum participant who identified herself as an employee of the EU Commission's Office for Internet Governance pointed out that many of the issues discussed during the forum were known risks that are acceptable to many in the name of greater cybersecurity. She further suggested that governments lacked sufficient incentive to reverse course, particularly after having invested significant resources in building higher technological fences. Zhou acknowledged the difficulties in reversing course but cautioned that internet fragmentation may slowly lead to economic loss in the form of lost efficiency. Over time, the sunk costs of abandoning, for example, national firewalls would pale in comparison to the economic losses from internet inefficiencies. He proposed that the path forward involves cost sharing between the government and major private sector ISPs and balancing security with technical efficiency.

DETAILED SCENARIO BREAKDOWN: A FRAGMENTED WORLD

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
1	17	Fragmentation has exponentially increased the rates of internet service disruptions and transfer errors, especially for cross-border data transfers.	**DP:** What critical infrastructure sectors might be most sensitive to internet service disruptions or transfer errors? Does it matter if only a small percentage of overall internet traffic is affected?
2	22	Thus, issues that apply to cross-border data transfer can affect even "domestic" industries.	**INFO**: Web services, such as email services, often host data in multiple caches in more than one country to ensure data availability and reliability. Web services that store millions of gigabytes of data may split data among any number of shards and distribute, copy, and back up data across multiple machines. This helps support a web service's goals for performance and efficiency—load balancing, for instance, can be even more efficient if the network chooses which "shards" of data need to be copied and distributed based on demand.
3	26	Industries that depend on rapid global internet connectivity (financial services, manufacturing, entertainment, etc.), for example, face rising costs and increasing downtime, as well as greater difficulty accessing real-time data.	**INFO**: Some additional impacts might include: ▪ Issues receiving updates on foreign-made software. ▪ Difficulty ensuring that real-time data is as up to date as possible. ▪ Problems with governments data exchanges. ▪ Difficulty tracing global shipments across differing internets. Impacts on e-commerce, manufacturing, agriculture, wholesale trade, and global pharmaceuticals as components come from all over the world.
4	29	…by separating their networks from the global internet, autocratic rulers have additional power to censor their citizens and prevent the free flow of information	**CONCERN:** Geopolitical risk; increasing risk of global instability and flash points. **INFO:** This is only one aspect of digital authoritarianism, which involves the use of digital information technology to surveil, repress, and manipulate domestic and foreign populations.
5	35	Competition in standards setting between the U.S. and China	**NOTE:** Both Scenario 1 and Scenario 4 also discuss standards and the resultant impact on technology development. Scenario 1 describes how a lack of security standards for cloud infrastructure and IoT devices presents considerable challenges for cybersecurity. Scenario 4 takes an alternate approach of discussing how voluntary standards adopted by industry may improve certain technologies.
6	42	China is throwing its weight behind international trade and standards-setting organizations that are more susceptible to its growing political influence and away from independent bodies such as the International Organization for Standardization (ISO).	**CONCERN:** Geopolitical and economic risks to the U.S.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
7	49	…the U.S. targeted AI and connectivity (5G, Wifi 6, and rural Wi-Fi access), enabling major advances in automation and IoT.	**NOTE:** Both Scenario 1 and Scenario 4 also cover technological advancements that enable major advances in IOT and automation. Scenario 1 discusses how these advancements reduce privacy, whereas Scenario 4 covers some of their more positive impacts.
8	52	China doubled down on its earlier successes in 5G, surveillance technology, and quantum communications. These investments continued to yield dividends for China, as well as the many Belt and Road Initiative countries and African authoritarian regimes that China exported its technology to.	**INFO:** The Belt and Road Initiative is a collection of infrastructure investment initiatives—stretching from East Asia to Europe—designed to expand China's economic and political influence. Referred to as the Digital Silk Road, China provides Chinese technology exports (e.g., Huawei's 5G technology), political support, and other assistance to Belt and Road countries.
9	61	…liberal Western democracies failed to pay sufficient attention to the internet's well-known insecurities, instead allowing private sector interests to dominate internet governance.	**NOTE:** Lack of internet regulation, particularly related to data collection and privacy, has been a competitive advantage to many U.S. tech companies, enabling surveillance capitalism. Additionally, a lack of collective action has prevented internet service providers from adopting more secure practices separate from government regulation.
10	65	…The Great Takedown, the cybersecurity event that would spark changes in internet governance around the world…	**NOTE:** Both Scenario 1 and Scenario 4 also cover a major cyberattack. Scenario 1 focuses more on attacks committed against individuals. Meanwhile, Scenario 4 discusses the physical impacts and geopolitical implications of cyber operations, as well as cyber espionage.
11	69	For years, China had been hacking the Border Gateway Protocol (BGP) to conduct state-sponsored espionage of all types, including man-in-the-middle attacks and hijacking traffic, rerouting data through government-aligned ISPs in China where they could view and potentially manipulate data.	**INFO:** China uses Points of Presence belonging to Chinese ISPs in North America to reroute and hijack legitimate traffic from the smaller networks that make up much of the larger internet, enabling them to intercept and view data traffic, steal passwords, and inject malicious code.
12	70	BGP issues take place daily and cause small outages, but usually are not noteworthy.	**INFO:** In the vast majority of cases, these incidents happen because of configuration mistakes and are resolved in minutes or hours.
13	72	…indiscriminately redirected a large segment of the internet through a government-owned ISP in China for nearly an hour.	**INFO:** The ISP can do this by "advertising" a more efficient route for traffic than is already available, regardless of whether or not the route actually exists. The more efficient the route advertised, the more traffic that will be routed through it.
14	77	…a plan to get all U.S. ISPs to collectively adopt more secure operating standards, in the hope that other ISPs worldwide will follow suit.	**NOTE:** This might be accomplished through an Internet Engineering Task Force (a multi-stakeholder body composed mainly of industry representatives), which would define protocols and standards for the ISP industry.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
15	86	…as well as growing concerns about cybersecurity, several nations instituted measures designed to flex their digital independence:	**NOTE:** Arguments in favor of segmentation are often multipronged. In addition to cybersecurity concerns, countries may be motivated by geopolitical concerns, privacy, economic benefit, and cultural concerns.
16	88	…protectionist policies to prop up domestic technology supply chains	**NOTE:** Protectionist policies are designed to favor domestic suppliers over those that are most efficient or effective. The European Union has recently initiated a series of policies designed to promote European Tech Champions as a means to compete with the U.S. and China.
17	89	…data localization requirements	**INFO:** ▪ Localization requires that all or part of the data on a country's citizens or critical sectors be stored within the country. ▪ In the past few years, more than 70 countries have passed new or updated data privacy laws that include some form of data localization. ▪ Widespread data localization could make many web services technically unviable because of the ways in which data is stored in caches around the world.
18	104	Storms, heat waves, and sea level rise increasingly threaten the physical infrastructure of the internet, including thousands of cables, data centers, points of presence, landing stations, and internet exchange points.	**INFO:** According to a 2018 study by University of Oregon and University of Wisconsin-Madison researchers, by 2030, 771 point of presences, 235 data centers, 53 landing stations, 42 internet exchange points, and 1,186 miles of fiber optic cable in the U.S. will be affected by a one-foot rise in sea level. New York, Miami, and Seattle will be the most heavily affected cities.

SCENARIO #3: DEEP DISINFORMATION

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

BRIEF DESCRIPTION

In the next five years, social divides that currently exist within the U.S. are exacerbated by more convincing disinformation campaigns (e.g., deepfakes, profiling) that are designed and targeted specifically to individual audiences through social media feeds. Mis-, dis- and malinformation (MDM) campaigns are rampant, disseminating fabricated or inaccurate information about a number of public health and safety issues and increasingly including calls to action that put public safety and critical infrastructure security at risk. MDM campaigns, fueled by increasingly sophisticated artificial intelligence and online tracking and data gathering, drive an increase in partisanship and the emergence of fringe groups more inclined to take action. Advances in AI-based tools also show promise in countering disinformation.

SCENARIO CONTEXT

- Sets up as two news reporting segments providing commentary on a recent domestic terrorism attack by a fringe extremist group that also employed deepfakes to spread disinformation in the aftermath. The commentary provides historical context for what transpired.
- Depicts a future emphasizing truth decay in the face of repeated and opportunistic use of disinformation and some ramifications that reduce public confidence in government institutions.
- Highlights the key role of AI-based technologies in both promoting and defending against MDM.
- Lays out competing interests influencing potential policy and regulatory decisions pertaining to the gathering of online data and its use.

FACILITATION QUESTIONS – TAILORED

Please note: Broader, more general facilitation questions—common to all four scenarios—are located in the Scenario Breakouts section of this facilitator's guide. Additional discussion points, as tied to specific potions of the scenario narrative, are listed in the scenario's "Detailed Scenario Breakdown."

- What underlying drivers are facilitating the emergence of extreme fringe groups? Are certain critical infrastructure sectors more susceptible to violent activity stemming from fringe conspiracies?
- How do issues related to public trust and social cohesion affect the functioning of critical infrastructure systems in daily operations and emergencies?
- What are the strategic needs to combat growing capabilities and the ease of spreading, targeting, and improving fake information?
    - How best can the federal government assist?
    - How do these trends influence current efforts to address violent extremism?

AMERICAN PUBLIC RADIO

APR's Jamie Muñoz talks first with Dr. Jacqueline Strickland, chief scientist at the Stenbirk Artificial Intelligence Research Consortium and then with former FBI Director Terrance Ford about the terror attack in Denver, efforts to counteract deepfake videos, and investigations into prior Russian disinformation campaigns.

Chief Scientist From SAIRC Discusses AI-based Technology That Showed Radiation Scare in Denver Was a Sophisticated Fake

April 24, 2026/4:40 PM EDT

Heard on *Considering Everything That's Happened*

Transcript

Jamie Muñoz, host: Two days ago, downtown Denver was rocked by an explosion outside the Byron G. Rogers Federal Building that killed five people, injured hundreds more, and damaged or destroyed dozens of buildings. The American Patriots, an extreme fringe group that first emerged three years ago, took immediate credit for the explosion. The group also posted several videos indicating that the explosion had released a dangerous amount of radiation into the air. [1] The videos went viral, prompting panic and gridlock as people tried to flee the Denver metropolitan area. Drew Hall from our Denver radio affiliate reported yesterday about the huge number of "worried-well" residents who flocked to area hospital emergency rooms and urgent care centers thinking that they had been exposed to radiation, severely overloading regional medical capabilities. [2] Since then, the Denver Fire Department, the Colorado State Patrol, and specialists from the U.S. Environmental Protection Agency and Department of Energy have all released preliminary reports finding no indications of a radiological release. However, many residents continue to express doubts about the results from initial environmental monitoring efforts [3] and are pushing hard on local, state, and federal officials for proof that the videos are fake.

Earlier this afternoon, the Stenbirk Artificial Intelligence Research Consortium—or SAIRC—posted the results from their analysis, which showed with 99 percent certainty that the videos posted by the American Patriots were sophisticated fakes. [4] Dr. Jacqueline Strickland, chief scientist at SAIRC, joins us from her office in Alta Palo. Welcome Dr. Strickland and thank you for joining us. What can you tell us about the work your organization has done to investigate and counter the viral videos posted by the American Patriots?

Dr. Strickland: Thank you for having me. The Stenbirk Artificial Intelligence Research Consortium is a public-private partnership between Stenbirk University, the Ethical AI Foundation, the National Science Foundation, and Radcleft National Laboratory dedicated to developing ethical uses of artificial intelligence—or AI. [5] Among other things, SAIRC's researchers have been investigating AI-based technologies for several years now as a way to identify flaws and inconsistencies that are inherent to even the most sophisticated "deepfake" videos. [6]

Jamie Muñoz, host: The videos released by the American Patriots after the explosion in Denver show first responders shouting about their radiation pagers going off, doctors treating what appear to be victims of radiation poisoning, and bodies of deceased radiation victims being sealed in body bags and placed in trucks. How did SAIRC determine that the videos were fakes?

Dr. Strickland: Our program was able to determine with over 99 percent confidence that all of the videos purporting to show evidence of radiation following the explosion in Denver were faked. Our latest program builds on prior research that trained AI networks to detect minute audio and visual inconsistencies that would not be visible to the naked eye, such as blinking patterns, distorted facial features, and mismatches between the sounds people make when speaking and the shapes of their mouths. The AI-based program we used to analyze the American Patriots videos also looks for subtle inconsistencies in how a person's expressions, tone, and composure should change based on the information they are providing or receiving.

Jamie Muñoz, host: Like if a person tells you a funny joke, but his voice is monotone and his face doesn't show any expression.

Dr. Strickland: Yes, exactly. The human eye is normally quite good at identifying these inconsistencies—we've all seen videos in which we know something is off, but we can't quite place what it is. But our ability to rely on our own built-in lie detectors to assess videos began to break down in the late 2010s. [7] The combination of more sophisticated, AI-based software programs and readily available apps made it easy to generate videos that couldn't be easily identified as fakes. [8] The SARS-19 deepfake videos in 2021 were the first instance in which a number of reputable news agencies were fooled into believing that they were true stories. [9] There were numerous video testimonials from medical professionals about how the vaccine didn't work and false narratives about high risks of permanent, debilitating side effects. These testimonials were based on real medical professionals whose images and voices were manipulated in wholesale fashion to generate fake videos. Other fake videos targeted extremely sensitive issues.

Jamie Muñoz, host: I remember APR reporting on the video about Edie Germaine, an ICU nurse from New York City, who was purported to have died from the SARS-19 vaccine. In fact, she had died tragically from a brain aneurysm.

Dr. Strickland: These videos were very effective in sowing distrust about the SARS-19 vaccine, which slowed vaccine uptake and ultimately prolonged the social and economic turmoil resulting from the pandemic. [10] According to polls at the time, as much as 33 percent of the U.S. population accepted the fake videos as true, even after a Justice Department investigation traced many of them to a multipronged disinformation campaign conducted by the Russian government. These videos were flagged by social media platforms as false or misleading or even removed, only to be reposted by others. [11] It was at this time that my colleagues and I recognized the need to develop an AI-based capability to identify and counter deepfake videos—to use AI to beat AI.

Jamie Muñoz, host: That was Dr. Jacqueline Strickland, chief scientist at SAIRC, which has shown that the radiation scare in Denver was a sophisticated hoax, hopefully bringing additional peace of mind to Denver residents. Dr. Strickland, thank you so much for talking with us.

Dr. Strickland: My pleasure. Thank you for having me.

Former FBI Director Provides Update on Denver Terror Attack and Discusses the History of Disinformation Campaigns and Deepfake Videos

April 24, 2026/4:45 PM EDT

Heard on *Considering Everything That's Happened*

Transcript

Jamie Muñoz, host: We are joined now by former director of the Federal Bureau of Investigation, Terrance Ford. Director Ford headed the FBI from 2022 to 2025 and oversaw several investigations into deepfake videos and disinformation campaigns that were traced back to the Russian government. Sir, thank you for joining us today. As the dust settles, what do we really know about the events in Denver?

Terrance Ford: Thank you for having me. Although the investigation is ongoing, what I can tell you is that the fringe group calling themselves the American Patriots took responsibility for the explosion two days ago in downtown Denver. They apparently used a nondescript panel truck to deliver the explosives. Minutes before the explosion, witnesses reported hearing a warning coming from the truck that highly radioactive materials would be released into the area. Just after the explosion, videos surfaced of first responders at the scene shouting in alarm that their radiation pagers were going off. Soon thereafter, other videos of doctors treating victims of radiation poisoning began to circulate. The result was a citywide panic, with officials scrambling to warn the public about a radiological attack that we now know had in fact not happened. Meanwhile, the Department of Energy and Environmental Protection Agency radiation response teams, which were meant to reassure the public that there was no radiation, arrived in full protective gear to conduct radiation tests. This led to further confusion and more outlandish theories among social media groups, stoking the public's fears about radiation, distrust in the government, and lack of confidence in nuclear safety institutions and fueling rumors about a federal cover-up.

Jamie Muñoz, host: Who are the American Patriots? What can you tell us about them?

Terrance Ford: We first learned about the American Patriots back in 2023. They were responsible for viral videos that purported to show illnesses arising from a contamination incident at a water treatment plant servicing an under-resourced community in the Milwaukee region. Another deepfake video provided undercover footage of senior plant operators and public officials, linking the incident to cost-savings measures and displaying an attempted cover up. The later deepfake, initially attributed to the American Patriots, was ultimately traced to Russian hackers who were opportunistically building on the American Patriots videos to create more confusion and distrust. [12] In a joint press conference, a spokesperson from the plant and an official from the public health department both vehemently denied the accuracy of these videos, and experts from the private sector and the Justice Department confirmed that they were sophisticated fakes. But far left- and right-leaning news organizations and social media groups continued to spread misinformation to their listeners, relying heavily on powerful algorithms to ensure that their groups got only the story they wanted to tell, effectively generating echo chambers that reinforced preexisting beliefs. [13] The American Patriots, for example, flooded their followers with "proof" that those affected in the videos were real and results showing the water was safe to drink were fake, emphasizing an underlying government conspiracy and inflaming tensions within the community.

Jamie Muñoz, host: You mentioned Russian hackers, and Dr. Strickland in our previous segment brought up the Russian government–sponsored disinformation campaign that prompted millions of Americans to

forgo the SARS-19 vaccine. Is there any indication that the Russian government is behind this attack or supporting the American Patriots?

Director Ford: Although we don't have any indication of Russian involvement in the videos posted following the Denver terror attack, we do know from experience that the Russian government sees polarization among Americans as a good thing and has become very effective in using micro-targeting to spread disinformation to individuals, pushing them further into their echo chambers. [14] Take for example the disinformation campaign two years ago that played off fears of both illegal immigration and another pandemic, with videos and interviews of immigrant caravans from Mexico and Central America carrying infectious diseases to the U.S. southwest border. [15] Frankly, we didn't know what to believe when presented with realistic-looking videos showing diseased people massing across the border from San Diego and El Paso and what looked like U.S. Border Patrol agents deploying tear gas and beating asylum-seekers. There were numerous calls to close the southern border. We saw protests and counter-protests in major cities across the U.S. and left- and right-leaning fringe groups became more violent in response to what they believed was happening. [16]

From the Russian perspective, their efforts were a monumental success, as these videos definitely affected the national public discourse and the views of lawmakers on Capitol Hill. Not only did it lead to protests, but it also influenced the passage of legislation reducing the numbers of allowed legal immigrants, including H1-B visas. Several lawmakers felt pressured to do something to assuage their constituents' concerns.

The Russians have a mature capability to sow discord through disinformation [17] and if they sense an opportunity, they'll seize on it. Remember the conspiracy theory that linked 5G towers to the spread of SARS-19; disinformation campaigns played on these fears, which eventually led to attacks on 5G infrastructure. Something similar happened with data centers. The Russians spread stories about data localization trends preventing companies from building data centers in cooler climates and linked this to exponential growth in energy consumption. They incited fringe environmental groups to try and sabotage data centers in the U.S. by convincing them that these centers posed an unprecedented environmental threat. Time and time again we've seen the Russians use disinformation as a means for it to punch above its weight class. Russians identify the fringes and fissures in society and encourage them to grow. Micro-targeting and deepfakes are just one set of tools in their disinformation efforts to undermine U.S. stability and cause us to focus more attention domestically.

Jamie Muñoz, host: Is there anything we can do to limit the effectiveness of these disinformation campaigns?

Director Ford: There's a common thread in the Justice Department investigations into the SARS-19 vaccination, water contamination incident, and southern border disinformation campaigns—these videos were targeted toward specific people and groups. The campaigns used sophisticated AI technology that gathers information on people by harvesting data from third-party cookies, location services, and user profiles. [18] Congressional action is needed to regulate the gathering of online data that allows malicious governments and fringe groups to prey on those most susceptible [19] to believing in the credibility of deepfake video messages and imagery, information that has damaged the fabric of our nation.

Jamie Muñoz, host: Congress is set to debate a bill to do just that next week. But its supporters are facing an uphill battle. IT companies that use this data to improve services and advertisers that use this data for targeted ads are already gearing up to fight this legislation in its current form. [20]

Director Ford, thank you for joining us this afternoon.

DETAILED SCENARIO BREAKDOWN: DEEP DISINFORMATION

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
1	18	The American Patriots, an extreme fringe group that first emerged three years ago took immediate credit for the explosion. The group also posted several videos indicating that the explosion had released a dangerous amount of radiation into the air.	**CONCERN:** Domestic extremists driven by fringe conspiracies; disinformation campaigns using deepfakes to incite panic and distrust of public institutions. **NOTE:** The authors elected to explore the use of disinformation in the context of a radiological dispersal device (RDD), as fear is a critical element in determining the short- and long-term impacts of an RDD event and makes it especially challenging to counter malicious disinformation.
2	22	…gridlock as people tried to flee the Denver metropolitan area. Drew Hall from our Denver radio affiliate reported yesterday about the huge number of "worried-well" residents who flocked to area hospital emergency rooms and urgent care centers thinking that they had been exposed to radiation, severely overloading regional medical capabilities.	**NOTE:** The authors identify two examples of how disinformation surrounding an RDD could affect critical infrastructure systems—namely, transportation and healthcare. **DP:** What other critical infrastructure systems could be affected in this scenario?
3	26	…many residents continue to express doubts about the results from initial environmental monitoring efforts…	**INFO**: Public trust is diminished when negative events occur involving topics that are not well understood by anyone other than subject matter experts. Past research has revealed a perception gap when it comes to radiation risks. **NOTE**: Part of what the authors wanted to explore was how public trust in institutions would affect potential situations with ramifications for critical infrastructure systems.
4	30	the Stanford Artificial Intelligence Research Consortium—or SAIRC—posted the results from their analysis, which showed with 99 percent certainty that the videos posted by the American Patriots were sophisticated fakes.	**NOTE**: As a point of reference, Facebook sponsored a 2019 Kaggle competition to detect deepfake videos. When tested against a set of previously unseen deepfakes, the winning algorithm was only capable of catching two-thirds of them. **DP**:

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
			▪ Do you expect the SAIRC announcement to sway public perception any better than the environmental monitoring efforts referenced earlier in the narrative? If so, why? ▪ What level of certainty do you believe the technology would be necessary to achieve in order to be beneficial? What other actions could be employed (either in response or in preparation to this type of incident) that might lead to greater public confidence?
5	37	… dedicated to developing ethical uses of artificial intelligence—or AI.	**NOTE:** Scenario 4 also introduces ethical AI as a tool to rapidly fact check information and debunk "fake news."
6	39	…SAIRC's researchers have been investigating AI-based technologies for several years now as a way to identify flaws and inconsistencies that are inherent to even the most sophisticated "deepfake" videos.	**NOTE**: As AI-algorithms to detect deepfakes improve, experts expect corresponding improvements to the AI-algorithms used to generate the deepfakes. Experts also disagree on whether AI-based technologies are the most effective counter to deepfakes. For example, one study disrupted the AI "learning" process by inserting noise that is undetectable by the human eye into a digital photograph **DP**: ▪ If this "cat and mouse" evolution continues, what other actions do you see as necessary to combat the risks presented by deepfakes? ▪ Do you see any circumstance occurring in the near term that might disrupt this evolution and lead to an advantage for one side over the other? ▪ Are there lessons learned from fighting other technological-based criminal activities that follow a similar pattern (e.g., computer viruses, malware, etc…)? What is the role of CISA in supporting efforts to disrupt deepfake capabilities?
7	57	The human eye is normally quite good at identifying these inconsistencies—we've all seen videos in which we know something is off, but we can't quite place what it is. But our ability to rely on our own built-in lie detectors to assess videos began to break down in the late 2010s.	**INFO**: The first application, FakeApp, that allowed users to manipulate and share videos with swapped faces was launched in January 2018. Less sophisticated videos are often easily identified as fake. As AI-based software improves, however, the subtle differences outlined in the previous paragraph—such as blinking patterns and distorted facial features—are becoming harder for the naked eye to recognize.
8	58	… readily available apps made it easy to generate videos that couldn't be easily identified as fakes.	**CONCERN**: Democratization of deepfake technologies that could be employed for nefarious purpose.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
9	60	The SARS-19 deepfake videos in 2021 were the first instance in which a number of reputable news agencies were fooled into believing that they were true stories.	**NOTE**: The authors wanted to provide another signal of the improvements in deepfake quality. **DP**: ▪ What additional concerns might arise from the amplification provided by mainstream media? ▪ Alternatively, what are the ramifications for mainstream media from a public trust standpoint? Is there a role for the federal government in helping the media validate information? Is there a role for CISA?
10	70	These videos were very effective in sowing distrust about the SARS-19 vaccine, which slowed vaccine uptake and ultimately prolonged the social and economic turmoil resulting from the pandemic.	**INFO**: According to a December 2020 survey by Pew Research Center, 60 percent of Americans say they would definitely or probably get a vaccine for SARS-19 if it were available today; this has fallen from 72 percent in May, but up from 51 percent in September. **NOTE**: Highlights another case study on the consequences of low public trust. **DP**: What are the ramifications of a slower economic recovery and return to "normal" for critical infrastructure resilience and security?
11	74	These videos were flagged by social media platforms as false or misleading or even removed, only to be reposted by others.	**INFO**: ▪ Facebook, for example, is the most common social media site used for news (43 percent of U.S. adults) but is struggling with misinformation and disinformation. A 2019 University of Oxford study found that despite the company's efforts, Facebook remains the number one social network site for disinformation and its use spreading disinformation is growing. Sympathetic trolls will reload content in the wake of its removal leading to greater persistence of information. For example, Facebook removed 1.5 million re-postings of the live-streamed video of the 2019 Christchurch, New Zealand, mosque shootings in the first 24 hours after the attack.
12	112	The later deepfake, initially attributed to the American Patriots, was ultimately traced to Russian hackers who were opportunistically building on the American Patriots videos to create more confusion and distrust.	**INFO:** Disinformation from bad actors can capitalize on public anxiety. In December 2014, for example, Russian trolls used Twitter to spread disinformation about police fatally shooting an unarmed black woman. This hoax followed protests over the shooting of Michael Brown.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
13	118	But far left- and right-leaning news organizations and social media groups continued to spread misinformation to their listeners, relying heavily on powerful algorithms to ensure that their groups got only the story they wanted to tell, effectively generating echo chambers that reinforced preexisting beliefs.	**INFO:** Recommending content to user groups with a shared characteristic (e.g., political affiliation, race, religion) can create echo chambers that affect societal discourse and norms. **DP**: ▪ How effective have CISA's efforts been in promoting educated consumers of information? What current challenges do these efforts face and how might they be resolved? What other options do government agencies have, given the sheer volume of misinformation and disinformation that can circulate?
14	128	…we do know from experience that the Russian government sees polarization among Americans as a good thing and has become very effective in using micro-targeting to spread disinformation to individuals, pushing them further into their echo chambers.	**CONCERN**: Use of micro-targeting to enhance disinformation campaigns **NOTE:** Scenario 1 also addresses micro-targeting by the Russian government, in this case to compromise military servicemembers through a series of cyber and physical attacks. **NOTE:** Scenario 4 also includes several instances of Russian-sponsored cyber attacks.
15	131	…played off fears of both illegal immigration and another pandemic, with videos and interviews of immigrant caravans from Mexico and Central America carrying infectious diseases to the U.S. southwest border.	**DP**: Having identified these sensitive and polarizing issues, what can the U.S. government and other stakeholders do to prepare for disinformation campaigns on these issues?
16	136	…left- and right-leaning fringe groups became more violent in response to what they believed was happening.	**CONCERN:** Violent attacks in response to disinformation campaigns **INFO:** Two additional factors from 2020 indicate the risk of future protests turning into civil unrest. First, armed individuals are now appearing more frequently at protests—between May and December 2020, observers have reported armed individuals at more than 50 demonstrations across the U.S. The August 2020 incident in Kenosha, Wisconsin, highlights the potential for rapid escalation to violence in these situations. Second, protests are now more frequently being met by counter-protests: Between May 24 and August 22, 2020, the U.S. Crisis Monitor recorded more than 360 counter-protests. Of these, 43 turned violent, with pro-police demonstrators clashing with Black Lives Matter demonstrators. Further, the insurrection at the U.S. Capitol on January 6, 2021, showed how a comprehensive disinformation campaign can incite a violent response.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
			DP: Given these trends, what steps can CISA take to support government agencies in ensuring that peaceful protests do not devolve to civil unrest?
17	142	The Russians have a mature capability to sow discord through disinformation…	**DP**: Russia sees polarization with the U.S. as a good thing, highlighted by the examples in the scenario. Are there steps CISA can take to protect those individuals who used to be moderate but are pushed by sophisticated disinformation campaigns fueled by micro-targeting into entering echo chamber environments?
18	159	The campaigns used sophisticated AI technology that gathers information on people by harvesting data from third-party cookies, location services, and user profiles.	**CONCERN**: With a growing consumer digital footprint, data from third-party cookies, location services, "fingerprinting," pre-built user profiles, etc. allow interested parties to micro-target users and tailor disinformation campaigns.
19	160	Congressional action is needed to regulate the gathering of online data that allows malicious governments and fringe groups to prey on those most susceptible…	**NOTE:** Scenario 4 includes passage of the Digital U.S. Act to protect user privacy, increase security, and build data governance structures. Scenario 1 also explores the impacts of a continued negative privacy trend.
20	165	Congress is set to debate a bill to do just that next week. But its supporters are facing an uphill battle. IT companies that use this data to improve services and advertisers that use this data for targeted ads are already gearing up to fight this legislation in its current form.	**INFO**: Companies collect data for monetization purposes ranging from training AI algorithms to sending customers promotional emails to predict and/or shape their future behaviors. **DP**: ▪ Given that companies design their business model around surveillance capitalism, what courses of action do you believe would be successful in preventing micro-targeting for nefarious purposes? How successful do you feel a legislative approach will be? What needs to be including in the legislation?

SCENARIO #4: A NEW WAVE OF COOPERATION

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

BRIEF DESCRIPTION

Following an international treaty in 2023 to improve collaboration in cyberspace, private companies see an opportunity to seek improvements in data sharing, interoperability, privacy, and security. Increasing international cooperation, combined with U.S. government efforts to overhaul its digital practices as well as its laws and regulations governing data privacy, help roll back the cyber sovereignty trend, spur greater technological innovation, and encourage ethical use of these innovations. However, the new wave of cooperation contributes to a relative decline in power for some countries, including one state actor that reacts by increasing its cyber-espionage operations.

SCENARIO CONTEXT

- Set as a podcast with interviews of key players highlighting major events in history leading to the era of digital cooperation both globally and between public and private sectors. The scenario provides a "things will get worse before they get better" context for how global and private-sector cooperation is brought about. It encompasses a period of time in which escalation of cyber-incidents into quid pro quo acts among state-based entities leads to effects on critical infrastructure systems and concerns over a "mutually assured disruption" environment.
- Highlights international, U.S. government, and private-sector efforts to address cyber norms and data privacy, data governance, and interoperability challenges.
- Provides an opportunity to discuss various "gray zone"[1] issues such as information warfare, proxy operations, cyber exploitation, and economic warfare.
- Depicts a future in which conditions accelerate technological advancements. One result is a reduced threat from disinformation, which in turn is linked to improved trust in institutions.
- Describes some potential longer-term ramifications to digital security arising from a global pandemic and major hack.

FACILITATION QUESTIONS – TAILORED

Please note: Broader, more general facilitation questions—common to all four scenarios—are located in the Scenario Breakouts section of this facilitator guide. Additional discussion points, as tied to specific potions of the scenario narrative, are listed in the scenario's "Detailed Scenario Breakdown."

- What do you see as other potential drivers that would lead to an escalation of cyber risks and the arrival at a state of "mutually assured disruption," as described in the narrative?
- What do you see as the respective roles that the public and private sectors play in addressing cybersecurity, data security, and data privacy?
- How do issues related to social trust, both within communities and throughout society, affect operations of critical infrastructure systems?

[1] Adversaries do not wish to engage the U.S. in direct military conflict, where their military and economic power would be overmatched. Instead, they employ activities in the "gray zone" that are designed specifically to slowly weaken the foundations of U.S. power and erode U.S. global dominance, but stop short of triggering a military response.

YEARS IN THE MAKING PODCAST TRANSCRIPT

TITLE: "CCC and D-USA: A new wave of cooperation among unlikely allies"

Hosted by Philippa Roth; produced by Naveen Mehta, Sandra Chung, and Greg Jackson

Monday, October 25, 2026

Philippa Roth (PR): Hello and welcome to the "Years in the Making" podcast from the *Phoenix Post,* where we discuss how past world events built to significant turning points in history in retrospect. I am your host Philippa Roth, and today we will be talking about the new wave of cooperation occurring in cyberspace—including data security, interoperability, standardization, and digital identity—that we've witnessed over the past three years between countries, members of Congress, and private sector companies.

We're joined by Jacques Viltard, the former U.S. Ambassador to the European Union, and Dr. Naomi Marmer, a national security analyst focusing on technology and cyberwarfare at the Center for Analysis of Security and Peace in Washington, D.C. Both played key roles in negotiating the Cooperation in the Cyberspace Convention (CCC). Ambassador Viltard also testified before Congress on a hearing focused on digital privacy prior to the passage of the Digital U.S. Act.

Ambassador Viltard, Dr. Marmer, thank you for joining us today.

Jacques Viltard (JV): Thank you for having me.

Naomi Marmer (NM): It's great to be here.

PR: So let's get right to it: How did we get here? If we turn back the clock to the beginning of this decade, I think some of the things our listeners may remember most are the SARS-19 pandemic, political polarization in the U.S., strained trade relations with China, and Black Lives Matter. Coming from what seemed to be such troubling and divisive times, how did we end up in a "golden" period of global cooperation that we arguably haven't seen since the twentieth century? Ambassador Viltard, perhaps we can start with you.

JV: Certainly. I think we have a classic case of "things will get worse before they get better" here. A few events come to my mind, starting of course with the SARS-19 pandemic. I would like to acknowledge first that the SARS-19 pandemic, like Hurricane Katrina in 2005, like the September 11 attacks in 2001, forced us to be more introspective as a nation. The hundreds of thousands of deaths, the rapid spread of the virus in certain communities and industries, the long-term economic ramifications of public health orders, and the distribution of vaccines brought out the already-present socioeconomic disparities. What people sometimes forget now is that the SARS-19 pandemic also represented a turning point for our reliance on the internet. [1] You had a sudden surge in remote work and online learning, both of which presented new targets of opportunity for malicious actors. [2] We saw large-scale cyberattacks on hospitals and schools that left thousands without access to critical care and compromised student data. [3] Once the widespread SARS-19 vaccine rollout began in 2021, there was a series of ransomware attacks on vaccine distributors by Fancy Bear in the U.S., EU, Brazil, and Canada. [4] While all of this was happening, the U.S. was figuring out how to respond to the Multiplicities hack. [5]

PR: Yes, the Multiplicities hack was one of the most extensive breaches at the time, compromising many government agencies and private companies. Dr. Marmer, how did the U.S. react to the hack?

NM: You know, at the time, the U.S. reaction was fairly by the book: The President imposed additional sanctions against Russia and froze accounts of oligarchs close to Putin to put Russia under further financial strain. The State Department also expelled diplomats and pressured allies to do the same. [6]

PR: So nothing out of the ordinary.

NM: No, and all of this made sense—they viewed Multiplicities as a classic act of espionage, which the U.S. also engages in when it is in our self-interest. You'll recall the U.S. and Israel interfering in Iranian nuclear operations over the years. A few prominent U.S. policymakers were initially advocating for a more retaliatory approach to the Multiplicities hack, but nothing really came of it [7]—at least, nothing publicly known. These are all calculated moves. The U.S. ran the risk of escalating things further and revealing our cyber arsenal. Public polling at the time showed that the country was against a retaliatory approach to Multiplicities because no one saw any tangible impacts of the hack on life or property. It wasn't until Russia interfered with Ukraine's natural gas supply in 2022 that Russia finally crossed the line. [8]

PR: That's right. What led Russia to act this way? And how did the international community respond?

JV: At the time, Putin was under tremendous political strain. Russia was feeling the burden of sanctions and still trying to recover from the SARS-19 pandemic. So as a way to distract the Russian people and rally support, Russia inflamed tensions with several adversaries, such as interfering with Ukraine's natural gas supply. This left the EU scrambling to meet its energy needs for a number of days. Unfortunately, the attack didn't trigger a united NATO response because Russia acted through a cyber-espionage group with close ties to its military to leave room for plausible deniability. [9] Putin maintained that some rogue actors were to blame, but as far as I am concerned it was very clear from forensic evidence that it was Russia. No hackers have sufficient incentive—let alone funds and resources—to engage in an attack of this scale and difficulty without state sponsorship.

NM: The Ukraine hack and the resulting energy disruptions were really a step too far for many world leaders. Once Europe as a whole visibly saw and felt the impact of the Ukraine cyberattack on its day-to-day operations, countries like Germany and France adopted Russia's middleman playbook and began to engage in a deliberate yet measured tit-for-tat response against Russia. For example, there was a cyberattack in the Ysyk-Ata district of Kyrgyzstan, where a Russian airbase is located, that left the district without power for 48 hours. This went largely unnoticed by news media, but definitely signaled to Putin that the West was no longer going to tolerate Russian intrusions.

I believe it created a broad appreciation that the world was in a "mutually assured disruption" environment, where if such tit-for-tat cyberattacks were to continue escalating, everyone was set up to lose. [10] This brings us back to Ambassador Viltard's "things will get worse before they get better" point. This prompted the U.S., Russia, China, the EU, and UK to negotiate and sign the Cooperation in Cyberspace Convention in 2023, codifying norms against nation-state cyberattacks. The CCC is really an important convention because it set redlines, created a forum through which countries could address cyber disputes, and established a sort of collective accountability that didn't exist previously. [11]

PR: That's really interesting. So it was the environment of "mutually assured disruption" we found ourselves in that served as an opening for unlikely bedfellows to come together and sign a convention.

I want to move to a different area of cooperation: the 2023 International IT Experts Forum. Ambassador Viltard, could you walk us through why the forum even took place and why it's seen as so instrumental to improving technology and user experience?

JV: Definitely. Your listeners might have noticed emails from various service providers detailing improvements to data privacy and security standards, interoperability changes, and the like. All of this is a result of the forum. For decades, the private sector, especially multinational corporations, has struggled to maximize the use of its data because each country had established its own unique set of data privacy, cybersecurity, and data governance requirements. [12] In the past five years alone, data localization efforts by the EU and India have been creating a lot of headaches when it comes to international data transfers and slowing down service. [13]

I believe the ratification of CCC signaled to the private sector that this was an opportune time for change. So several of the major tech companies convened a forum with academics, ethicists, lawyers, and CIOs and after more than a month's worth of deliberation produced standards that increase interoperability and data sharing among companies, integrate differential privacy, improve security, and promote ethical use of data. [14] These, of course, were voluntary standards and not as strong as any government directive. But to the surprise of many of us, enough companies did agree to start phasing in these standards so that by 2024 they reached a critical mass. [15] User security and privacy have increased dramatically over the past few years and I expect to see additional benefits moving forward.

PR: Yes, experts have applauded the forum, saying it has acted in tandem with the Digital U.S. Act to protect user privacy, increase security, and provide other benefits. I'd particularly like to get your thoughts here, Dr. Marmer.

NM: I think that's a fair assessment. D-USA, which is essentially our national data security and privacy protection law, adds the government-directive element, at least for American firms, which Ambassador Viltard was referring to. Passage of D-USA has been significant for several reasons: one, it is a testament to the new cooperative efforts we've seen across the political aisle and among countries and industries over the past few years. If you told me in 2020 that we'd have an American version of the General Data Protection Regulation by 2023, I wouldn't have believed you because of the sheer gridlock and disagreement over key issues, such as user control over personal data, regulation of third-party data brokers, and so on. [16] The International IT Experts Forum ended up resolving some of these disagreements for Congress with a collective, industry-wide move toward standardization. Take differential privacy, for instance. This would have been a highly contested issue, but congressional members didn't need to negotiate much to protect the interests of organizations operating in their jurisdictions because these companies were already in agreement with one another on the path forward. [17]

Additionally, D-USA, took the recommendations of the 2020 Cyberspace Solarium Commission report to heart, and set out to overhaul the government's privacy and data security regime and allocate resources to achieve these goals. This was a direct response to the Multiplicities hack, which was a colossal failure of U.S. cyber defense systems. Congress realized the extent to which U.S. government agencies and critical infrastructure companies were lagging behind in their data security, privacy, and governance efforts. So it created a National Cybersecurity Assistance Fund to provide funding for research and created additional opportunities for public-private collaboration in these fields, one of which is the four-year employee exchange between tech companies and government agencies. [18]

PR: Yeah, I think the public has taken to this effort quite well, especially the digital identity cards and how much they've helped improve customer service.

JV: I agree. And for your listeners who might not have received their digital identity card yet—they are a part of the privacy and security regime overhaul we've been discussing. Many Americans started to receive them a year ago. They have been pointed to as having helped reduce red tape, get easier access to government services, and resolve disputes with agencies more quickly. [19] I suspect a full rollout will

also address issues ranging from identity theft to helping provide a smoother TSA experience at the airport.

PR: Would you agree that this new cooperative environment, coupled with increased research funding, has accelerated improvements in 6G, IoT, and AI-enabled technologies? [20]

JV: Yes, definitely. The advancement in those technologies also benefited from the 2020 antitrust lawsuits in the U.S. and Europe against FaceMe and Dongle. Since then, companies have largely stayed away from predatory practices, such as acquiring emerging competitors, to remain under the Justice Department's radar and avoid scrutiny. So the tech industry benefitted from smaller companies being able to raise funds, recruit talent, and use a number of high-quality datasets, which were made available following the forum and D-USA. All of these factors really helped diversify the tech sector by lowering the barriers to entry and enabling more innovation in 6G, AI, and IoT.

The diversification of the tech industry and increase in public funding have stimulated what I call "public good" advancements. Take the company Ethical AI, for instance, which provides algorithms to news media groups for fact checking, allowing them to debunk fake news much more quickly. [21]

NM: Think about what that's done for our understanding and acceptance of truth and facts in the U.S.!

PR: That's a great point. I think it was a recent survey from the Khumalo Research Center that reported increased public trust in government institutions for the first time since the 1980s. Do you think these largely positive trends we have been discussing will continue?

NM: As much as I would like to give a definitive "yes," there are many areas in which the U.S. government and its allies have work to do. Take Iran, for instance. I briefly touched on the U.S. and Israel interfering in Iran's nuclear operations. I can tell you Iran isn't very happy; it's still recovering from the economic downturn resulting from the pandemic, struggling to control additional SARS outbreaks within its borders, and frustrated over sanctions. So I suspect it will be a thorn in the U.S.'s side over the coming years.

JV: That's right—Iran is becoming nervous about its declining power in the Middle East, especially as more countries begin to normalize relations with Israel. Iran is looking to flex its muscles and reassert its dominance in the region. We've already seen it copy China and carry out cyber-espionage operations to advance its tech sector by stealing intellectual property and to destabilize other countries, especially Iraq and Saudi Arabia. [22] But I remain optimistic that the international community will remember what happened in Ukraine and prevent things from escalating further.

PR: Well, thank you both so much for your time. It's been a really interesting conversation. We hope to have you again on the show.

JV: It's been a pleasure.

NM: Thank you.

DETAILED SCENARIO BREAKDOWN: A NEW WAVE OF COOPERATION

Please note: The version of the narrative that the facilitator possesses has line numbers for ease of identifying key segments of the scenario narrative (as referenced in the table below). These segments are also highlighted in green and labelled with reference numbers.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
1	32	…the SARS-19 pandemic also represented a turning point for our reliance on the internet.	**INFO**: ▪ A survey of CFOs by Gartner found that 74 percent of organizations plan to shift some employees to remote work permanently. The general Internet activity also spiked, with some studies citing a 47 percent increase in internet use in 1Q20 compared to 1Q19.
2	33	You had a sudden surge in remote work and online learning, both of which presented new targets of opportunity for malicious actors.	**INFO**: ▪ According to the Bureau of Labor Statistics, 35 percent of U.S. workers teleworked because of the pandemic in May 2020 (the first month for which statistics were reported), including 56 percent of government workers. ▪ As of Sep 2, 73 of the 100 largest school districts in the U.S. are starting the school year in remote-learning only. ▪ 52 percent of U.S. adults who are newly working from home because of SARS-19 use personal laptops for work—often with no new tools to secure it; 45 percent have not received new training. **NOTE:** Scenario 1 also explores a continued remote work trend, but from the perspective as a driver of new technologies (e.g., IoT enables devices).
3	35	We saw large-scale cyberattacks on hospitals and schools that left thousands without access to critical care and compromised student data.	**INFO**: For example, Universal Health Services was hit by a ransomware attack in September 2020, affecting many of its more than 400 healthcare facilities across the U.S. and Great Britain. This month also saw the first death directly attributed to a ransomware attack, as a woman in Germany with a life-threatening condition was denied admission to a Düsseldorf hospital experiencing a ransomware attack and sent to another hospital.
4	36	…a series of ransomware attacks on vaccine distributors by Fancy Bear in the U.S., EU, Brazil, and Canada.	**INFO**: Fancy Bear (aka, APT28), is a team of hacker working for Russia's Main Intelligence Directorate (GRU). The group has been held responsible for attacks

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
			such as the 2016 breaches of the Democratic National Committee and the Clinton campaign.
5	37	While all of this was happening, the U.S. was figuring out how to respond to the Multiplicities hack.	**NOTE:** Scenario 1 and Scenario 2 also cover a major cyberattack, however Scenario 1 focuses more on cyber and physical attack on the U.S. military, while Scenario 2 focuses more on the financial impacts and geopolitical implications.
6	42	The President imposed additional sanctions against Russia and froze accounts of oligarchs close to Putin to put Russia under further financial strain. The State Department also expelled diplomats and pressured allies to do the same	**NOTE**: The moves are akin to those imposed on Russia for its interference in the 2016 presidential election and in response to the March 2018 poisoning of a former Russian double agent, Sergei Skripal, living in Britain.
7	47	…they viewed Multiplicities as a classic act of espionage, which the U.S. also engages in when it is in our self-interest. You'll recall the U.S. and Israel interfering in Iranian nuclear operations over the years. A few prominent U.S. policymakers were initially advocating for a more retaliatory approach to the Multiplicities hack, but nothing really came of it…	**INFO:** ▪ An analysis by the Cyber Unified Coordination Group, which is composed of the FBI, CISA, ODNI and NSA, shows that the hack was carried out by a Russian actor and compromised a number of U.S. government agencies and private sector companies. ▪ Attackers entered government systems as early as Fall 2020, but the government only learned of the hack in December 2020, when FireEye, a private cybersecurity company, came forward. Hackers were able to gain access through SolarWinds's compromised software updates and establish additional backdoors and cover their tracks.
8	52	It wasn't until Russia interfered with Ukraine's natural gas supply in 2022 that Russia finally crossed the line.	**NOTE**: Although the narrative mentions later on that "the attack didn't trigger a united NATO response," one issue that the authors wanted to explore was the notion of redlines. It remains unclear, for example, what form a cyber-attack would have to take and required severity that would lead to NATO invoking Article 5 of the North Atlantic Treaty, which states that an attack on an Ally or Allies shall prompt collective defense from the Alliance. **DP**: What considerations would you incorporate into defining redlines for grey zone conflicts when it comes to attacking critical infrastructure?
9	59	…Russia inflamed tensions with several adversaries, such as interfering with Ukraine's natural gas supply. This left the EU scrambling to meet its energy needs for a	**CONCERN**: While not explored in this scenario, one emerging threat is the increased rate of attacks and widened source of advanced cyber threats to the government, military, and critical infrastructure facilities from Internet

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
		number of days. Unfortunately, the attack didn't trigger a united NATO response because Russia acted through a cyber-espionage group with close ties to its military to leave room for plausible deniability.	mercenaries. Internet mercenaries are highly trained ex-intelligence officers that make their skills available to the highest bidder. This means that nation state–level cyber capabilities are put into the hands of small nations, companies seeking strategic advantage, and other non-state actors. Click here for additional information.
10	72	…countries like Germany and France adopted Russia's middleman playbook and began to engage in a deliberate yet measured tit-for-tat response against Russia. For example, there was a cyberattack in the Ysyk-Ata district of Kyrgyzstan, where a Russian airbase is located, that left the district without power for 48 hours. This went largely unnoticed by news media, but definitely signaled to Putin that the West was no longer going to tolerate Russian intrusions. I believe it created a broad appreciation that the world was in a "mutually assured disruption" environment, where if such tit-for-tat cyberattacks were to continue escalating, everyone was set up to lose.	**NOTE:** The narrative takes inspiration from the Cold War era military doctrines of deterrence and "mutual assured destruction," which theorize that because use of nuclear weapons by two or more adversaries would mean complete annihilation of the world, no side has the incentive to start such a conflict. Our growing reliance on the internet for crucial services (i.e., banking, employment, educational, and medical) and the convergence of operational technology and informational technology (i.e. connecting electric power grids to the Internet) means that a cyberattack on critical infrastructure could significantly *disrupt* our economy, national security, and the ability to go about daily life.
11	76	…the Cooperation in Cyberspace Convention in 2023, codifying norms against nation-state cyberattacks. The CCC is really an important convention because it set redlines, created a forum through which countries could address cyber disputes, and established a sort of collective accountability that didn't exist previously.	**NOTE**: Holding actors accountable through international arbitration is often difficult, especially when norms or laws have not been codified. Even though only a handful of countries are named as signatories of the CCC in this scenario, the signing of the convention is a step towards addressing the concerns (one of which is the absence of a cyberwar treaty) of legal scholars and diplomats.
12	86	…the private sector, especially multinational corporations, has struggled to maximize the use of its data because each country had established its own unique set of data privacy, cybersecurity, and data governance requirements.	**INFO**: ▪ Privacy compliance has become a major cost center for some companies. In a November 2019 PwC survey, 52 percent of tech, media, and telecom respondents ranked data privacy among the top three policies that impact their businesses the most. ▪ Many countries (European countries, India, Vietnam) 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.

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
			▪ Cyber sovereignty includes data nationalization, which can take several forms: o Mirroring: requiring that copies of certain data be stored in-country. o Data localization mandates: requiring that certain data be stored in a specific geographic area in a specific way. o Foreign access limitations: reducing actual or perceived foreign access to data through technical or legal means. Content control: controlling and limiting content dissemination online.
13	88	…data localization efforts by the EU and India have been creating a lot of headaches when it comes to international data transfers and slowing down service.	**INFO:** Recent bills put forth in India lay out a fourth model—the Global South model—for global data governance, in comparison to the Chinese, U.S., and EU models. The Global South model is partially motivated by a desire to push back against concerns about U.S. tech influence and exploitative data collection practices. The extent to which India's current efforts can attract other countries (e.g., Brazil) to adopt its model will be critical over the next few years in shaping the global privacy landscape.
14	93	…the major tech companies convened a forum with academics, ethicists, lawyers, and CIOs and after more than a month's worth of deliberation produced standards that increase interoperability and data sharing among companies, integrate differential privacy, improve security, and promote ethical use of data.	**DP**: The narrative only speaks to the forum's efforts at a high level. Are there any specific concerns such a forum would ideally address that you would like to discuss further? **NOTE:** Both Scenario 1 and Scenario 2 also discuss standards and the resultant impact on technology development. Scenario 1 describes how a lack of security standards for cloud infrastructure and IoT devices presents considerable challenges for cybersecurity. Scenario 2 focused on competition in standards setting between the U.S. and China.
15	95	…voluntary standards and not as strong as any government directive. But to the surprise of many of us, enough companies did agree to start phasing in these standards so that by 2024 they reached a critical mass.	**DP**: In this scenario, the authors purposefully took a more optimistic view on the success of voluntary standards, even as the narrative later introduces D-USA. ▪ What is your reaction to this viewpoint? What conditions are necessary for voluntary standards to be more successful?
16	107	D-USA, which is essentially our national data security and privacy protection law, adds the government-directive element, at least for American firms, which Ambassador Viltard was referring to. Passage of D-USA has been significant for several reasons: one, it is a testament to	**DP**: ▪ What are some of the other barriers to passing D-USA? How would you see D-USA differing from GDPR?

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
		the new cooperative efforts we've seen across the political aisle and among countries and industries over the past few years. If you told me in 2020 that we'd have an American version of the General Data Protection Regulation by 2023, I wouldn't have believed you because of the sheer gridlock and disagreement over key issues, such as user control over personal data, regulation of third-party data brokers, and so on.	
17	112	Take differential privacy, for instance. This would have been a highly contested issue, but congressional members didn't need to negotiate much to protect the interests of organizations operating in their jurisdictions because these companies were already in agreement with one another on the path forward.	**INFO**: ▪ Differential privacy is a mathematical property that processes can have. A differentially private analysis guarantees that anyone seeing the result will make the same inference, regardless of whether a specific individual's private information is included as an input. The advantage of differential privacy is that it mathematically guarantees protection against a wide range of privacy attacks. ▪ Although Dwork et al. first outlined the concept of differential privacy in 2006, very little legal pressure or market incentive exists for companies to invest in differential privacy. For instance, Google and Facebook have not prioritized solving the technical problems associated with building out a differential privacy platform. An effort by Uber in 2017 to create such a platform to support data analytics while protecting customer privacy was unsuccessful in arriving at a solution that could be generally applied. If these market and legal trends continue, inconsistent development of differential privacy in the private sector may result. **DP**: ▪ What do you see as the best ways to accelerate development of robust tools for differential privacy and ensure their broad accessibility? What other promising alternatives to de-identification do you see that are currently underdeveloped?
18	120	Additionally, D-USA, took the recommendations of the 2020 Cyberspace Solarium Commission report to heart, and set out to overhaul the government's privacy and data security regime and allocate resources to achieve	**INFO:** The Cyberspace Solarium Commission was established to "develop a consensus on a strategic approach to defending the U.S. in cyberspace against

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
		these goals. This was a direct response to the Multiplicities hack, which was a colossal failure of U.S. cyber defense systems. Congress realized the extent to which U.S. government agencies and critical infrastructure companies were lagging behind in their data security, privacy, and governance efforts. So it created a National Cybersecurity Assistance Fund to provide funding for research and created additional opportunities for public-private collaboration in these fields, one of which is the four-year employee exchange between tech companies and government agencies.	cyber- attacks of significant consequences." Its final report included over 80 recommendations organized into 6 pillars: 1. Reform the U.S. Government's Structure and Organization for Cyberspace. 2. Strengthen Norms and Non-Military Tools. 3. Promote National Resilience. 4. Reshape the Cyber Ecosystem. 5. Operationalize Cybersecurity Collaboration with the Private Sector. 6. Preserve and Employ the Military Instrument of National Power. **CONCERN:** ▪ A rise in copy-cat "supply chain attacks," in which hackers hijack trusted software updates provided by legitimate companies to break into their customers' networks. ▪ The hackers stole FireEye's sophisticated cyber defense and offensive tools and could use these to carry out future cyberattacks. ▪ Hackers were able to view Microsoft's source code and gain access to various companies' Microsoft 365 email services and Azure Cloud infrastructure, making code manipulations appear legitimate and taking control of certificates and keys used to generate authentication tokens (also known as SAML tokens). **NOTE:** SolarWinds outsourced operations to Eastern Europe, where operators are more vulnerable to Russian pressures, to cut costs and has evaded basic security protocols. SolarWinds has also come under scrutiny for using proprietary code rather than industry partial open-source code for its updates, which prevented coders outside of the company from identifying vulnerabilities. **DP**: ▪ What do you envision as key components of D-USA? ▪ What are the most critical research needs at this time?
19	126	… their digital identity card yet—they are a part of the privacy and security regime overhaul we've been discussing. Many Americans started to receive them a year ago. They have been pointed to as having helped reduce red tape, get easier access to government	**INFO**: Digital identity cards are used for physical and digital identification, verifying the card holder in the real world and online. They are used for online transactions, accessing government services, traveling, digitally signing documents, and even voting. These identification cards provide security through transparency and by

Ref No.	Line #	Narrative Reference Text	Additional Comments DP: Discussion Point INFO: Additional Information NOTE: Clarification/Rationale CONCERN: Potential issue, threat, or vulnerability
		services, and resolve disputes with agencies more quickly.	keeping a digital footprint (i.e., activity log). Some ID cards, such as Estonia's, also provide the holder access to information held about them online. **DP**: What are the risks and benefits of a digital identity system for critical infrastructure security and resilience?
20	130	Would you agree that this new cooperative environment, coupled with increased research funding, has accelerated improvements in 6G, IoT, and AI-enabled technologies?	**DP**: For brevity and storytelling purposes, the narrative does not include an expansive discussion on the ramifications of these technologies. What might be some risks that emerge with the adoption of these technologies? **NOTE:** Scenario 1 and Scenario 2 also discuss the benefits associated with technological enhancements, specifically advances in IoT and 5G, although in Scenario 2, these advances are undercut by other technological issues.
21	140	The diversification of the tech industry and increase in public funding have stimulated what I call "public good" advancements. Take the company Ethical AI, for instance, which provides algorithms to news media groups for fact checking, allowing them to debunk fake news much more quickly.	**DP**: Are there other applications of AI valuable for critical infrastructure resilience and security that you feel are languishing right now because of inadequate financial return on investment? If so, what do you see as potential mechanisms for increasing interest in developing these applications? **INFO**: A key finding from a 2018 RAND report, Truth Decay, is that the online content to which individuals are exposed shapes their perception of facts. This is problematic, given the presence of misinformation and disinformation online, particularly on social media platforms. **NOTE**: For brevity and storytelling purposes, the narrative does not include an expansive discussion on the trust in government institutions, which is featured to a greater extent in Scenario #3. However, if time permits, you may want to explore this issue with the group.
22	154	So I suspect it will be a thorn in the U.S.'s side over the coming years….That's right—Iran is becoming nervous about its declining power in the Middle East, especially as more countries begin to normalize relations with Israel. Iran is looking to flex its muscles and reassert its dominance in the region. We've already seen it copy China and carry out cyber-espionage operations to advance its tech sector by stealing intellectual property and to destabilize other countries, especially Iraq and Saudi Arabia.	**NOTE**: In addition to balancing the tone of the narrative and closing out the podcast, the authors wanted to provide an opportunity for participants to discuss their concerns regarding foreign adversary grey zone attacks and how they might evolve in the future.

APPENDIX A: WORKSHOP PLANNING CONSIDERATIONS

Step 1: Set a target date for the event at least three months in advance.

Step 2: Identify workshop staff.

Staffing the workshop requires a time commitment from at least eight individuals—four facilitators and four document leads. Facilitators should expect to spend at least 30 hours on the workshop, and document leads, at least 15 hours. In addition, a workshop coordinator should expect to spend 10–15 percent of his or her time in the three months prior to the event in organizing the workshop and engaging with invitees. Workshop planning efforts may also require periodic input from a planning committee (e.g., to tailor the workshop goals).

Step 3: Identify potential invitees.

A scenarios workshop requires 40–50 participants. Thus, hosts may need a list of 55–70 candidates to secure the necessary number of participants. When identifying candidates, the workshop sponsor/planning committee/coordinator should target the following groups:

- Mid-to-senior career-level individuals interested in exploring longer-term risks to critical infrastructure to enable effective risk mitigation.
- A mix of representatives (e.g., CISA personnel; state and local planners; fusion center personnel; private-sector representatives; subject matter experts from non-profits, think tanks, and academia).
- Individuals with interest and expertise in anonymity and privacy, data storage and transmission, and trust and social cohesion.
- Individuals familiar with strategic foresight.

Because the virtual workshop divides participants into four breakout rooms (one for each scenario), consider the best way to achieve a mix of different perspectives and expertise among the groups when identifying candidates. The workshop coordinator should tap into the networks of the Regional Director, senior leaders, Protective Security Advisors, Cybersecurity Advisors, and members of the planning committee to identify participants. The workshop coordinator may also need to coordinate engagement efforts within the region to identify additional participants for the workshop. Thus, the workshop coordinator may want to develop and circulate a one-page flyer on the scenarios workshop. An example can be requested at SecureTomorrowSeries@cisa.dhs.gov.

As prospective participants are identified, it would be useful to record additional information about them in a spreadsheet to help prioritize invitations (and potential backup candidates). Possible data fields include the following:

- Name
- Position
- Organization
- Subject matter expertise in one or more of the topic areas (e.g., data storage and transmission, anonymity and privacy, trust and social cohesion)
- Stakeholder group (e.g., private sector, public sector, nongovernmental organization, academia)

- Experience/expertise in strategic foresight
- Link to professional bio

Step 4: Start sending invitations and tracking responses.

Roughly two months before the workshop, the workshop coordinator should begin issuing invitations and tracking RSVPs. Invitations should come from a senior leader within the sponsoring organization. Invitation language may require leadership review and coordination with the leader's executive assistant on invitation roll out. Candidates should send RSVPs to the workshop coordinator, who should respond immediately with a save-the-date meeting invitation.

Step 5: Review scenarios and identify key discussion points.

Each of the three topics addressed by the scenarios is broad, providing opportunities for hosts to tailor the workshop to their interests. Facilitators are unlikely to have time to address all the discussion points listed in the detailed scenario breakdowns. Thus, the workshop sponsor, planning committee, and coordinator should review the scenarios and select the key discussion points that facilitators should prioritize for the participants in their group. It may be useful to invite facilitators to participate in or observe these deliberations so they can gain a better idea of leadership intent and begin familiarizing themselves with the scenarios.

Step 6: Train the facilitators and document leads.

Five weeks prior to the workshop, the workshop coordinator should hold a meeting with all workshop personnel to walk through the agenda and train them on specific responsibilities and desired outputs of each session (using this facilitation guide as a reference). The coordinator should introduce each of the facilitator-document lead pairings at this time and give them their assigned scenarios (if they have not yet received them).

A second, follow-on meeting should be held for the facilitators to talk through their scenarios with one another and to receive additional training on workshop priorities. This meeting will help the facilitators to gain a more holistic understanding of the scenarios to help with Stress-Test Rounds and to discern the distinctions between different directions explored by each scenario.

Step 7: Determine scenario assignments.

Three weeks prior to the workshop, the workshop coordinator should finalize the assignment of attendees to scenarios. As noted earlier, because the workshop divides participants into four groups, consideration should be given to the mix and balance of different perspectives and expertise among the groups when making group assignments.

Step 8: Send out participant information.

Two weeks before the event, each participant should receive the following:

- Assigned scenario narrative
- One-page brief describing the four scenarios
- Workshop feedback form (optional)
- Are We There Yet? Participant Form (if receiving polling information beforehand)

- Participant biographical information

If participants are receiving a polling form, remind them to complete and return the form one week before the workshop to allow sufficient time for compiling and analyzing the results and updating the "Are We There Yet?" results slides.

Step 9: Make final preparations.

A few days before the event, conduct a final review of the slides, emphasizing transitions between speakers and between plenary and breakout sessions, and selecting files to share on the virtual meeting platform. During this review, the workshop coordinator should confirm assignments for supporting workshop sessions (e.g., who will be presenting/manipulating the slides, providing technical support, monitoring chat).

Hosting a virtual scenarios workshop is a major undertaking and can be considered a capstone activity that follows execution of matrix games or cross-impacts sessions. For additional details about the steps necessary to plan a virtual workshop, please see Appendix A: Workshop Planning Considerations.

Facilitators should review in detail the support materials that pertain to their assigned scenario. Although they should focus most of their attention on their assigned scenario, facilitators should also review the remaining scenarios.

Prior to the workshop, the workshop coordinator will assign participants (maximizing diversity of backgrounds in each group) to one of four groups. Each group will focus on one of the scenario narratives. Participants should receive their assigned scenario narrative at least one week before the workshop as a read ahead. Facilitators should review their list of assigned participants and familiarize themselves with the background and affiliation of each participant.

APPENDIX B: IN-PERSON WORKSHOP AGENDA

The scenarios workshop facilitation guide is written for a two-afternoon, virtual execution of the workshop. However, the workshop can also be configured as a one-day, in-person event (see below for alternative agenda). Unless otherwise indicated as plenary, the sessions occur in breakout groups.

TIME	ACTIVITY
8:00–8:30am	Registration
8:30–9:15am	Framing the workshop: welcome, participant introductions, workshop objectives, and roadmap for the day's activities (*plenary session*)
9:15–10:00am	Icebreaker exercise: Are we there yet? (*plenary session*)
10:00–10:15am	Break
10:15–12:15pm	Scenario breakouts • Scenario familiarization and build out • Identification of emerging and evolving risks and associated needs • Risk mitigation strategies
12:15–1:00pm	Lunch
1:00–1:10pm	Divide breakout group and prepare for stress-test rounds
1:10–1:55pm	Alternative future stress test: Round 1
1:55–2:40pm	Alternative future stress test: Round 2
2:40–2:55pm	Break
2:55–3:40pm	Alternative future stress test: Round 3
3:40–4:30pm	Synthesis and reflection (*plenary session*)
4:30–4:45pm	Closing remarks (*plenary session*)