Scenarios Workshop – Introduction and Roadmap Presentation Slide Notes

Slide 1

Cover slide that reads Scenarios Workshop – Introduction and Roadmap

Slide 2

Slide title, "What is Scenario-Based Planning?"

- Most strategic planning operates on the assumption that the future is simply a continuation of current trends. Strategic foresight explicitly forces us to challenge this assumption by considering a multiplicity of plausible futures.
- This workshop uses four scenarios 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.
- For the purposes of this workshop, a scenario is a story with plausible cause-and-effect linkages that connects a future condition with the present, while illustrating key decisions, events, and consequences throughout the narrative.
- Futurists make a distinction between plausible futures and all possible futures. Plausible futures are ones in which a reasonable audience, upon hearing a story about how the future comes about, can believe its validity.

Slide 3

Slide title is, "Goals of this Workshop"

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.

Slide 4

Slide title, "About the Scenarios"

- **Anonymity and privacy:** As the value of data grows, maintaining the balance between identity verification and protecting anonymity is becoming increasingly challenging with technological advances in artificial intelligence (AI) and proliferation of Internet of Things (IoT) devices, which present evolving threats to individual control of data and privacy.
- **Trust and social cohesion:** Social cohesion, or citizens' belief that they are part of a community and that fellow citizens, governing bodies, and institutions are invested in the well-being of that community, is being strained by foreign interference, political polarization, and disinformation, among other threats. As social cohesion deteriorates, it will be a source of potential risk to critical infrastructure.
- **Data storage and transmission:** Unprecedented rates of data generation is putting increasing emphasis on secure data storage and transmission. Data access, integrity, and confidentiality are critical to national functions, national security, and national competitiveness.

The names of the four scenarios are listed on the right. Just to provide you with a bit of context on each:

- Scenario 1, Life Under a Microscope, refers to the aftermath of a series of cyber and physical attacks on personnel from a nuclear power plant. The attacks are tied to foreign adversary's use of third-party data brokers.
- Scenario 2, A Fragmented World, highlights a more fragmented global internet and ramifications of decreasing security and reliability of data transfers.
- Scenario 3, Deep Disinformation, is about a recent domestic terrorism attack by a fringe extremist group that also uses deepfakes to spread disinformation in the incident's aftermath.
- Scenario 4, New Wave of Cooperation, highlights major historical events leading to the current era of digital cooperation both globally and between public and private sectors.

Slide 5

Slide title is, "Workshop Agenda". No notes.

Slide 6

Slide title is, "Day One: Icebreaker Exercise". No notes.

Slide 7

Slide title is, "Day One: Scenario Breakouts"

- After the break, we'll start with the scenario breakouts. The objectives here are to explore the scenario, reacting to and building on the narrative using your different expertise and perspectives; to understand how the scenario conditions will lead to emerging and evolving risks for critical infrastructure and to identify mitigation strategies for those risks; and to prioritize five risk mitigation strategies to increase security and resilience toward what occurs the scenario.
- The outputs will be a concrete, prioritized list of up to five recommended risk mitigation strategies to improve critical infrastructure resilience and security in the world that is described by your scenario. These strategies will feed into sessions on Day Two that stress-test the strategies against alternative future scenarios.

Slide 8

Slide title is, "Day Two: Stress-Test Rounds"

- Day One was narrowly focused on exploring the particular scenario you were assigned. Day Two broadens the aperture. We examine how future uncertainty further shapes the insights you arrived at yesterday. Participants will participate in three rounds of stress testing. By the end of these sessions, participants will have had their risk mitigation strategies assessed for robustness against all of the other workshop scenarios.

Slide 9

Slide title an image of the Cybersecurity and Infrastructure Security Agency (CISA) seal and logo