SECURE TOMORROW SERIES SCENARIOS WORKSHOP SYNOPSES

OVERVIEW

This workshop uses hypothetical scenario narratives to help participants explore ways in which the operating environment for critical infrastructure (CI) owners and operators may evolve over the next 5 to 10 years, and how this evolution may affect the security and resilience of CI 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. Brief descriptions of each workshop scenario are provided below.

SCENARIO #1: LIFE UNDER A MICROSCOPE

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 #2: A FRAGMENTED WORLD

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 #3: DEEP DISINFORMATION

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 (AI) 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 #4: A NEW WAVE OF COOPERATION

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.

For more details, please contact SecureTomorrowSeries@cisa.dhs.gov.