SECURE TOMORROW SERIES

OVERVIEW

The Cybersecurity and Infrastructure Security Agency's (CISA) Secure Tomorrow Series is a strategic foresight capability that examines emerging and evolving risks that could significantly affect our nation's critical infrastructure in the next 5–20 years. Secure Tomorrow Series strives to build a more resilient and secure future by bringing together groups of subject matter experts, thought leaders, and other stakeholders from diverse backgrounds to think proactively about future risks. Identifying these risks is essential to mitigating them before they affect critical infrastructure systems.

USING STRATEGIC FORESIGHT TO SECURE NATIONAL CRITICAL FUNCTIONS

A central premise of strategic foresight is that no one entity can successfully predict the future. Instead, the methodology treats the future as a set of plausible alternatives with the intent of identifying actions that, if taken today, would steer a community toward its preferred future. For CISA, this means a future in which the nation's critical infrastructure and the related National Critical Functions (NCFs) are more secure and resilient. In its role of identifying and reducing future risks, CISA's National Risk Management Center (NRMC) applies strategic foresight to identify risk mitigation strategies that are robust against uncertainty and uses this knowledge to promote methods for securing critical infrastructure systems that underpin the NCFs in the long term.

Secure Tomorrow Series efforts align with the NCFs approach to risk management. The NCFs are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

SECURE TOMORROW SERIES TOPICS OF EXPLORATIONS

In selecting topics for exploration under Secure Tomorrow Series, CISA sought those that are likely to influence multiple NCFs. The current focus is to develop the thinking surrounding the effects of the following three topics on critical infrastructure and cybersecurity:

Brain-Computer Interfaces (BCIs)

BCIs have long been confined to medical laboratory settings, where they have demonstrated enormous promise for helping patients regain motor function or communicate. In recent years, major technology companies have begun investing in BCIs, bringing an infusion of resources that will likely accelerate breakthroughs in BCI capabilities, more commercial applications, and their entry into numerous sectors. However, these advances will bring a host of potential privacy, security, equity, and individual welfare concerns. Additionally, other countries are investing in developing BCI technology, which may expose the United States to risks from economic and military competition, as well as ethical, legal, and security concerns.

NCFs include: Educate and Train, Preserve Constitutional Rights, Protect Sensitive Information, Provide Medical Care, Provide Wireless Access Network Services, and Support Community Health

Synthetic Biology

Synthetic biology is the redesigning and harnessing of biological organisms to impart new or improved abilities and produce products. In the next 5–20 years, synthetic biology will likely contribute to significant advances in food and agriculture, healthcare, sensors and diagnostics, manufacturing, and more. However, synthetic biology poses dual-use risks; the rapid progress in this field that is contributing to beneficial advances can also facilitate nefarious applications

such as making relatively benign bacteria and viruses more pathogenic. Manipulation of systems using synthetic biology could result in unintended or accidental negative impacts.
NCFs include: Manage Hazardous Materials, Manage Wastewater, Produce and Provide Agricultural Products and Services, Produce and Provide Human and Animal Products and Services, Produce Chemicals, Provide Medical Care, and Supply Water

Quantum Technologies (computing, communications, and sensors)

The rapid development of quantum technologies—specifically, quantum computers and new algorithms that can break public key encryption (PKE)—raises the specter of a potentially catastrophic future threat to all applications that depend on information and communications technologies. The risks are multilayered and entwined, and certain critical infrastructure systems are particularly vulnerable because of their reliance on internet-connected industrial control systems and internet-enabled distributed operations.
NCFs include: Provide Internet-based Content, Information, and Communication Services; Conduct Elections; Maintain Access to Medical Records; Protect Sensitive Information; Provide Consumer and Commercial Banking Services; Provide Identity Management and Associated Trust Support Services; Provide Information Technology Products and Services; and Research and Development

SECURE TOMORROW SERIES TOOLKIT

In December 2021, CISA began conducting research and analyses for each topic and engaging with SMEs from academia, think tanks, the private sector, and the U.S. Department of Energy's National Labs to develop knowledge products meant to encourage systems thinking; identify emerging risks; develop corresponding risk management strategies to implement now; and stress-test these strategies against multiple alternative futures.

One of the key knowledge products is the next iteration of the Secure Tomorrow Series Toolkit. The toolkit consists of supporting materials (e.g., facilitation guides, scenarios, game components) to help critical infrastructure stakeholders and planning communities' organizations conduct strategic foresight activities, support strategic planning, and be empowered to execute these methods to examine the three topics.

RESOURCES

- National Risk Management: CISA.gov/topics/risk-management
- National Critical Functions: CISA.gov/national-critical-functions
- Secure Tomorrow Series: CISA.gov/secure-tomorrow series
- Secure Tomorrow Series Toolkit: CISA.gov/secure-tomorrow-series-toolkit

For more information, contact us at SecureTomorrowSeries@cisa.dhs.gov.

Scan this QR to go to the webpage directly.