SECURE TOMORROW SERIES

SCENARIO NARRATIVE 2: A FRAGMENTED WORLD

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

UNITED NATIONS WORLD DATA FORUM: BUILDING THE GLOBAL INTERNET

Meeting in Brief

January 12–16, 2026

United Nations (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. 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.

Kapoor outlined some of the ways in which the fractured internet has affected critical industries. For example, industries that depend on rapid global internet connectivity (such as financial services, manufacturing, entertainment, etc.), face rising costs and increasing downtime, as well as greater difficulty accessing real-time data. Tracking commodities and shipments across the world has become more difficult. These challenges have also undercut investments in 5G and Internet of Things (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. 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: 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). 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 and connectivity (5G, Wi-Fi 6, and rural Wi-Fi access), enabling major advances in automation and IoT. 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. 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. 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, 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. BGP issues take place daily and cause small outages, but usually are not noteworthy. 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. 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.

- **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:

  - The EU implemented protectionist policies to prop up domestic technology supply chains.
  - India, Japan, and Indonesia passed data localization requirements.
  - 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. 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

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.