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: ○ Mirroring: requiring that copies of certain data be stored in-country. ○ Data localization mandates: requiring that certain data be stored in a specific geographic area in a specific way. ○ 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)

- 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*)