Share Your News Now

If you would like to share news or information with our readers, please send the unique stories, business news organization events, and school news to us includinig your name and phone number in case more information is needed.

For news and information consideration, please send to News@scdaily.com
or contact
John Robbins 281-965-6390
Jun Gai 281-498-4310

Southern DAILY
Make Today Different
Southern Daily News is published by Southern News Group Daily

Publisher: Wea H. Lee
President: Catherine Lee
Editor: John Robbins

Address: 11122 Bellaire Blvd., Houston, TX 77072
E-mail: News@scdaily.com

Inside C2

Sunday, March 26 2023

California farmers flood their fields in order to save them

HELM, California, March 24 (Reuters) - When Don Cameron first intentionally flooded his central California farm in 2011, pumping excess stormwater onto his fields, fellow growers told him he was crazy.

Today, California water experts see Cameron as a pioneer. His experiment to control flooding and replenish the ground water has become a model that policy makers say others should emulate.

With the drought-stricken state suddenly inundated by a series of rainstorms, California's outdated infrastructure has let much of the stormwater drain into the Pacific Ocean. Cameron estimated his operation is returning 8,000 to 9,000 acre-feet of water back to the ground monthly during this exceptionally wet year, from both rainwater and melted snowpack. That would be enough water for 16,000 to 18,000 urban households in a year.

"When we started doing this, our neighbors thought we were absolutely crazy. Everyone we talked to thought we would kill the crop. And lo and behold, believe me, it turned out great," said Cameron, vice president and general manager of Terra Nova Ranch, a 6,000-acre (2,400-hectare) farm growing wine grapes, almonds, walnuts, pistachios, olives and other crops in the San Joaquin Valley, the heart of California's $50 billion agricultural industry.

If more farmers would inundate their fields rather than divert precipitation into flood channels, that excess could seep underground and get stored for when drought conditions return.

California swings between disastrous drought and raging floodwaters. This season has been especially rainy, with 12 atmospheric rivers pounding California since late December, placing greater importance on flood control. More wet weather is forecast in the coming week.

Don Cameron stands next to one of his flood capture projects on his Terranova Ranch in Helm, California, U.S., January 25, 2023. REUTERS/Mike Blake

Terra Nova's basins are filled with 1.5 to 3.5 feet of water, Cameron said Wednesday. He plans to eventually flood 530 acres of pistachio trees and 150 acres of wine grapes plus another 350 acres that are planted only when excess floodwater is available.

The state Department of Water Resources provided $5 million and Terra Nova another $8 million for the project, which includes a pumping system. So far there has been virtually zero return for the company, Cameron said, though it may acquire future water rights for its groundwater contributions.

Cameron "is definitely what we call the godfather of on-farm recharge. He's really the pioneer who began doing it first," said Ashley Boren, CEO of Sustainable Conservation, an environmental group with a focus on supporting sustainable groundwater management.

This mimicking of nature - letting water flow across the landscape - is the most cost-effective way to manage peak flood flows, experts say, while banking the surplus for drier days.

"It's not only going to benefit us, it will benefit our neighbors," Cameron said.

Cameron began his 30-year-old passion project before the state passed the Sustainable Groundwater Management Act (SGMA) of 2014, a law that sought to avoid a looming disaster from overdrafts.

Since then, policy makers have worked on economic incentives for more farmers to follow suit. Some water districts that are responsible for implementing SGMA have offered growers credits toward water rights in exchange for recharge. Pending state legislation would simplify permitting and guarantee water rights for participating growers.

California Governor Gavin Newsom signed an executive order on March 10 making it easier for farmers to divert floodwaters onto their lands until June.

There is no statewide monitoring of on-farm recharge, but Sustainable Conservation is keeping track of four water districts in the San Joaquin Valley that recorded 260 farmers replenishing their aquifers this year, returning at least 50,000 acre-feet (61.7 million cubic meters) back into the ground as of mid-February.

California, which has a strategic goal of adding 4 million acre-feet of storage, recently provided $260 million in grants to Groundwater Sustainability Agencies established under SGMA. The state received applications seeking $800 million, indicating demand for projects, said Paul Gosselin, deputy director of the state's Sustainable Groundwater Management Office.

Besides cost, growers face other obstacles to on-farm recharge. A farm must have access to the water, cannot hurt endangered species and cannot flood land subjected to certain fertilizers or pesticides or dairy farm waste.

In the Merced River Watershed, willing farmers could recapture enough future floodwater to replace 31% of the groundwater they are overdrafting under existing conditions, said Daniel Mountjoy, director of resource stewardship for Sustainable Conservation, who participated in a state study. That could jump to 63% with changes in reservoir management and infrastructure improvements, he said.

To achieve sustainability throughout the San Joaquin Valley, an estimated 750,000 to 1 million acres of irrigated farmland would have to be fallowed, Mountjoy said.

"We're at the beginning of a lot of momentum for groundwater recharge programs," said Gosselin, of the state groundwater office. "The last two years (of extreme drought) was a wakeup call for everybody."

WEA LEE'S GLOBAL NOTES

03/24/2023

The Glory of Asian-Americans

KP George who was re-elected as Fort Bend County judge recently held a luncheon at the community center to welcome the Houston Consulate Corp. More than fifty diplomatic envoys from Asia, Africa and Europe attended the event and listened to the blueprint of the region's future.

Ft. Bend County, located near Houston's suburbs is the most ethnic area in the United States with a population of nearly 700,0000 in the Sugarland and Missouri City areas. It has been selected as one of the most livable areas in the nation.

Nearly twenty percent of the residents are Asian and because they are highly educated and work in the high-tech industry, the region has become one of the most prosperous economic areas in the country.

Our host Judge George is of the first generation of immigrants from India. He is diligent and understands the grassroots of our community. He understands the special needs of the residents in the region, so he was elected easily to a second term as judge.

Mr. Geroge, we are all very proud of you. Your success represents the contributions of our new immigrants to our society. It is only the very few politicians who discriminate against Asians who don't know about, or do not fully understand, the important value of our diversity.

Wea H. Lee
Wealee@scdaily.com
Chairman of International District Houston Texas
Publisher Southern Daily Wea H. Lee
Southern News Group Chairman / CEO
Chairman of International Trade & Culture Center
Republic of Guiana Honorary consul at Houston Texas

Southern DAILY Make Today Different

Editor's Choice

People walk near a damaged building in the aftermath of a deadly earthquake, in Kahramanmaras, Turkey. REUTERS/Suhaib Salem

Police officers shoot at a drone during a Russian drone strike in Kyiv, October 17, 2022. REUTERS/Vadim Sarakhan

Smoke rises after a Russian drones strike in Kyiv, October 17, 2022. REUTERS/Gleb Garanich

Two soldiers with the 58th Independent Motorized Infantry Brigade of the Ukrainian Army release a drone for a test flight near Bakhmut, Ukraine, November 25, 2022. REUTERS/Leah Millis

A Ukrainian serviceman takes cover as an air-raid siren sounds during a Russian drone strike, which local authorities consider to be Iranian-made unmanned aerial vehicles (UAVs) Shahed-136, in Kyiv, October 17, 2022. REUTERS/Gleb Garanich

European Council President Charles Michel and Ukrainian President Volodymyr Zelenskiy attend the European leaders summit in Brussels, Belgium. REUTERS/Yves Herman

Southern DAILY Make Today Different

BUSINESS

Former President Donald Trump Declared The COVID-19 Pandemic A National Emergency On March 13, 2020

President Biden Will End COVID Emergencies On May 11th

Compiled And Edited By John T. Robbins, Southern Daily Editor

President Joe Biden

(Photo/ Andrew Harnik/Associated Press

Key Point

The move to end the COVID national emergency and public health emergency declarations would formally restructure the federal coronavirus response to treat the virus as an endemic threat to public health that can be managed hrough the various agencies' normal authorities.

WASHINGTON — President Joe Biden informed Congress on Monday that he will end the twin national emergencies for addressing COVID-19 on May 11, as most of the world has returned closer to normalcy nearly three years after they were first declared.

The move to end the national emergency and public health emergency declarations would formally restructure the federal coronavirus response to treat the virus as an endemic threat to public health that can be managed through agencies' normal authorities.

It comes as lawmakers have already ended elements of the emergencies that kept millions of Americans insured during the pandemic. Combined with the drawdown of most federal COVID-19 relief money, it would also shift the development of vaccines and treatments away from the direct management of the federal government.

Former President Donald Trump Declared The COVID-19 Pandemic A National Emergency On March 13, 2020.

Biden's announcement comes in a statement opposing resolutions being brought to the floor this week by House Republicans to bring the emergency to an immediate end. House Republicans are also gearing up to launch investigations on the federal government's response to COVID-19.

Former President Donald Trump first declared the COVID-19 pandemic a national emergency on March 13, 2020. The emergencies have been repeatedly extended by Biden since he took office in January 2021, and are set to expire in the coming months. The White House said Biden plans to extend them both briefly to end on May 11.

"An abrupt end to the emergency declarations would create wide-ranging chaos and uncertainty throughout the health care system — for states, for hospitals and doctors' offices, and, most importantly, for tens of millions of Americans," the Office of Management and Budget wrote in a Statement of Administration Policy.

President Biden Received His Covid Vaccine During the Emergencies.

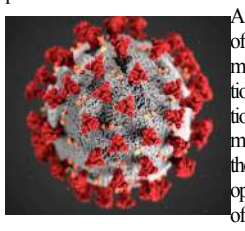
Congress has already blunted the reach of the public health emergency that had the most direct impact on Americans, as political calls to end the declaration intensified. Lawmakers have refused for months to fulfill the Biden administration's request for billions more dollars to extend free COVID vaccines and testing. And the $1.7 trillion spending package passed last year and signed into law by Biden put an end to a rule that barred states from kicking people off Medicaid, a move that is expected to see millions of people lose their coverage after April 1.

The costs of COVID-19 vaccines are also expected to skyrocket once the government stops buying them, with Pfizer saying it will charge as much as $130 per dose. Only 15% of Americans have received the recommended, updated booster that has been offered since last fall.

Once the emergency expires, people with private insurance will have some out-of-pocket costs for vaccines, tests and treatment, while the uninsured will have to pay for those expenses in their entirety.

Legislators did extend telehealth flexibilities that were introduced as COVID-19 hit, leading health care systems around the country to regularly deliver care by smartphone or computer.

The Biden administration had previously considered ending the emergency last year, but held off amid concerns about a potential "winter surge" in cases and to provide adequate time for providers, insurers and patients to prepare for its end.



A senior administration official said the three months until the expiration would mark a transition period where the administration will "begin the process of a smooth operational wind-down of the flexibilities enabled by the COVID-19 emergency declarations." The official spoke on the condition of anonymity to discuss the announcement before it had been released.

More than 1.1 million people in the U.S. have died from COVID-19 since 2020, according to the Centers for Disease Control and Prevention, including about 3,700 last week.

Case counts have trended downward after a slight bump over the winter holidays, and are significantly below levels seen over the last two winters — though the number of tests performed for the virus and reported to public health officials has sharply decreased.

Moments before the White House's announcement, Rep. Tom Cole, R-Okla., accused the president of unnecessarily extending the public health emergency to take action on issues like forgiving some federal student loan debts.

President Biden Will End COVID Emergencies On May 11th, 2023.

"The country has largely returned to normal," Cole said Monday, introducing a Republican-backed bill calling for an end to the health emergency. "Everyday Americans have returned to work and to school with no restrictions on their activities. It is time that the government acknowledges this reality: the pandemic is over."

Related

FDA Experts Urge Single Annual COVID Vaccine Formula For All, But Variants Are Still With Us. Recommendations Would Override The Original COVID Vaccine Mix.

A vial of the COVID-19 booster vaccine is shown to media at Santa Clara County Fairgrounds Expo Hall in San Jose, Calif., on Monday, Oct. 17, 2022. (Photo/ Shae Hammond/Bay Area News Group)

The original COVID-19 vaccine formula introduced in December 2020 should be retired and replaced entirely with the updated mix tailored to recent virus variants, an FDA expert panel urged in a unanimous vote this week.

The Food and Drug Administration's Vaccines and Related Biological Products Advisory Committee was asked to consider whether to recommend a single vaccine composition for all situations, the so-called bivalent formula based both on the original virus strain and the more recent omicron BA.4/5 strains.

"This isn't only a convenience thing to increase the number of people vaccinated, which is extremely important," said Dr. Hayley Gans, pediatrics professor at Stanford University Medical Center, during Thursday's panel discussion. "But also I think moving toward the strains that are circulating is important."

But COVID'S ever-evolving mutations make that difficult. Even the strains the updated booster shot was designed to protect against are rapidly vanishing. The Centers for Disease Control and Prevention indicates that the omicron BA.4 variant is no longer circulating and that BA.5 only represents about 2% of cases nationally, edged out by XBB.1.15, which now accounts for about half of infections.

"I do think it's important to get closer to the circulating strains," said Dr. Paul Offit, a pediatrics professor at Children's Hospital of Philadelphia.

It was unclear how soon the FDA might put the committee's recommendation into action.

The move comes as a succession of omicron variants of the virus that causes COVID-19 continues to infect the vaccinated, boosted and unvaccinated, but hospitalizations and deaths haven't soared as they did in past winter waves of infection since the virus emerged three years ago, in early 2020.

Last year, the FDA experts urged new booster shots based on both the original virus strain that emerged in Wuhan, China and some of the newer omicron virus variants, known as BA.4 and BA.5.

But that updated formula was only recommended for boosters to goose the immune response for the already vaccinated. Those who had not been vaccinated had to get the original vaccine, based on a now-extinct strain. Health officials said the original vaccine still showed strong protection against severe illness.

Experts have said low vaccination rates since then suggest the strategy wasn't popular. Currently, 61% of Americans and 75% of Californians have had the primary, two-dose COVID-19 vaccination. But only 15% nationally and 18% in California have had the single, updated booster shot unveiled last fall.

Others on the panel questioned the need for vaccines to combat infections that don't produce symptoms.

"You can certainly make the argument an asymptomatic infection is desirable," said Dr. Cody Meissner, a pediatrics professor at Dartmouth-Hitchcock Medical Center in Lebanon, New Hampshire, adding it will "act as its own boost."

"We certainly want to stop the virus from circulating," Meissner said. "But that's probably not going to be possible. The virus is always going to mutate and evolve and find ways to avoid the immunity humans build up."

During the open comment period, several people told the panel they had suffered severe side effects from the vaccines and felt the agency was downplaying the risks.

Angie Bluford, who said she's a 49-year-old mother from Wilmington, North Carolina, said she got the Moderna vaccine in April 2021 "to protect my family," thinking she was "doing the right thing," and that she felt ill the next day, with headaches, shortness of breath and other symptoms.

"My body is a shell of what it once was," she said. "Please hear us and help us."

Dr. Tom Shimabukuro of the CDC's immunization safety office said that the CDC is still investigating indications of a possible elevated stroke risk in older people that appeared in one of several safety monitoring networks and not others.

"The public and the medical community should be confident that the government has systems in place to rapidly detect safety problems," Shimabukuro said. "We are aware of these reports of people experiencing long-lasting health problems following COVID vaccination. No specific medical causes for the symptoms have been found. We will continue to monitor the safety of these vaccines."

The panel concluded with discussions about future vaccine and booster schedules and dosages but made no recommendations. (Courtesy mercurynews.com/)

Southern DAILY Make Today Different

COMMUNITY

The U.S. Has Announced Its National Cybersecurity Strategy: Here's What You Need To Know

Compiled And Edited By John T. Robbins, Southern Daily Editor

The White House, Washingron D.C. (Photo/Unsplash/David Everett Strickler)

Key Points

The White House released the new US National Cybersecurity Strategy in March 2023.

In 2022, the average cost of a cybersecurity attack was more than $4.5 million, according to IBM.

The new framework seeks to protect critical infrastructure, including hospitals and clean energy facilities, from cyber threats. It also aims to increase collaboration with international coalitions and partnerships to counter threats to the digital ecosystem.

The US government is continuing efforts to strengthen the country's cybersecurity prowess as well as bolster its overall technology governance strategy. Earlier this month, President Joe Biden released a new National Cybersecurity Strategy, which outlines steps the government is taking to secure cyberspace and build a resilient digital ecosystem that is easier to defend than attack — and that is open and safe for all.

"When we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable and secure," Biden wrote in the framework's preface.

The strategy is part of a larger effort by the Biden administration to strengthen cyber and technology governance. This included efforts to increase accountability for tech companies, boost privacy protections and ensure fair competition online.

Why does the US need a National Cybersecurity Strategy?

The world is increasingly complex and cyberthreats are growing more sophisticated, with ransomware attacks running into millions of dollars in economic losses in the US. In 2022, the average cost of a ransomware attack was more than $4.5 million, according to IBM.

The greatest risks we face are interconnected, creating the threat of a "polycrisis", whereby the overall combined impact of these events is greater than their individual impact. This is equally true of technological risks, where, for example, attacks on critical information infrastructure could have disastrous consequences for public infrastructure and health, or where growing geopolitical tensions heighten the risk of cyberattacks.

Cybercrime and cyber insecurity were seen by risk experts surveyed for the World Economic Forum's Global Risks Report as the 8th biggest risk in terms of severity of impact, across both the short term (next two years) and over the coming decade. In 2022, state-sponsored cyberattacks targeting users in NATO countries increased by 300% compared to 2020, according to Google data.

With cyberattacks on the rise, experts at the World Economic Forum's Annual Meeting at Davos predicted that 2023 would be a "busy year" for cyberspace with a "gathering cyber storm".

"This is a global threat, and it calls for a global response and enhanced and coordinated action," Jürgen Stock, Secretary-General of the International Criminal Police Organization (INTERPOL), said at Davos.

The Forum's Global Cybersecurity Outlook 2023 also found that 93% of cybersecurity experts and 86% of business leaders believe that global instability will have a negative impact on their ability to ensure cybersecurity over the next two years.

Robust cybersecurity is key to building on the promise of emerging technologies to enable growth and shared prosperity, while minimizing the perils they pose.

As Biden notes, "Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense.

"We must ensure the internet remains open, free, global, interoperable, reliable, and secure – anchored in universal values that respect human rights and fundamental freedoms."

What are the 5 pillars of the National Security Strategy?

The COVID-19 pandemic accelerated the world's digital transformation, which means we rely on connected devices and digital technology to do more than ever before – putting our lives and livelihoods at greater risk from cyberthreats.

The US' National Security Strategy recognizes the need to rebalance the burden of responsibility for cybersecurity away from small businesses and individuals and onto the public and private organizations best placed to defend cyberspace through "robust collaboration". It also seeks to build cyberspace resilience by balancing the need to address immediate threats, with incentivizing investment in the secure, long-term future of the digital ecosystem.

Each of the five pillars it sets out are broken down into strategic objectives, but here's a quick overview of what they entail:

1. Defend critical infrastructure To build confidence in the resilience of US critical infrastructure, regulatory frameworks will establish minimum cybersecurity requirements for critical sectors.

2. Disrupt and dismantle threat actors Working with the private sector and international partners, the US will seek to address the ransomware threat and disrupt malicious actors.

3. Shape market forces to drive security and resilience Grant schemes will promote investment in secure infrastructure, while liability for secure software products and services will be shifted away from the most vulnerable and good privacy practices will be promoted.

4. Invest in a resilient future A diverse cyber-workforce will be developed and cybersecurity R&D for emerging technologies including postquantum encryption will be prioritized.

5. Forge international partnerships to pursue shared goals The US will work with its allies and partners to counter cyberthreats and create reliable and trustworthy supply chains for information and communications technology.

Related

The Seven Trends That Could Shape The Future Of Cybersecurity In 2030

1. Progress in cybersecurity, but access must be widened

As technologies advance, so do the skills of hackers seeking to exploit system vulnerabilities.

Organizations need to understand cyber risks and plan for tomorrow's challenges.

We've outlined the trends which could shape the future of cybersecurity and how to prepare for them.

In order to disrupt a country, halt major commercial flows or make important financial gains, hackers usually look for vulnerabilities that have not yet been discovered. The constant technological evolution is a catalyst for them to find new flaws to exploit. Therefore, in a fast-evolving digital ecosystem, decision-makers in government, industry, academia, and civil society need to anticipate and address tomorrow's cybersecurity challenges to stay ahead of the curve.

Public and private investments in security technologies, as well as broader efforts to tackle cybercrime, defend critical infrastructure, and raise public awareness about cybersecurity, are likely to reap tangible payoffs by 2030. Cybersecurity will be less about "defending fortresses" than moving toward acceptance of ongoing cyber-risk, with a focus on bolstering resilience and capacity for recovery.

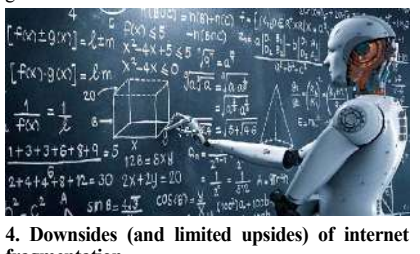
As markers of this trend, passwords could be nearly obsolete by 2030, cybersecurity will be widely taught in primary schools, and cryptocurrencies will be more effectively regulated. Still, while investments in more secure systems and basic cyber hygiene will raise many above the "cyber poverty line," progress is likely to be unevenly distributed across communities and geographies.

2. Worsening crisis in trust online

Erosion of trust online is poised to deepen and continue to undermine offline relationships and institutions. Advances in artifical intelligence (AI) and machine learning (ML) will make it increasingly difficult to distinguish between humans and machines online, potentially leading many people to shift their activities back offline and even revert to using analogue devices. In a world of increasingly sophisticated synthetic media and AI-based cyberattacks, cybersecurity will become less about protecting confidentiality and more about protecting the integrity and provenance of information. Unfortunately, at the moment when societies most need to come together to solve major problems like climate change, distrust could lead to a retreat from regional and global cooperation. We need to work to avoid this outcome.

3. Double-edged sword of AI and ML technologies

There is both optimism and uneasiness about the rapid pace of scientific advancement and commercial adoption of AI and ML technologies. On the upside, we will see vast innovation in sectors such as medicine and transportation, as well as improvements to cybersecurity. On the downside, AI will also lead to innovation in cybercrime, and ML models could train themselves to achieve illicit or devious ends. There is a lack of clarity in how governments, companies, or communities will ensure that AI and other technology-based systems are built, deployed, and monitored safely and ethically, and no clear forum from which that guidance will come.



4. Downsides (and limited upsides) of internet fragmentation

The trend toward "digital sovereignty" and internet fragmentation will continue, as efforts toward internet interoperability and cross-border data transfers will compete with efforts by governments to establish localized or regional controls over online spaces. This may be an opportunity for local communities to have more agency in defining digital security, but we could also see a "wild west" of disinformation, surveillance, and more powerful cyberattacks emanating from rogue states that have isolated themselves from the global internet. The trend toward deglobalization could also lead to more pronounced "regional pockets of truth," with differences in information defined by geographic or other boundaries, and governments could exert more control through technology.

5. Pull and push between regulatory experiments and the future of privacy

By 2030, we will know whether early cybersecurity efforts at privacy legislation (such as Europe's GDPR) are delivering on their policy objectives, but it remains uncertain whether we will have improved methods for managing personal data by 2030 or will be living in a world in which we have given up on contemporary notions of individual privacy.

6. Metaverse uncertainty

Participants were split between those who believe that the metaverse (or metaverses) will not materialize, and will be considered a failed experiment by 2030, and those who believe we need to accelerate policy innovation to keep up with the new privacy and security issues that a fully realized metaverse will pose. However, the most dystopian visions of the future that emerged from the workshops were based on a passive consumer (i.e., living in the metaverse to escape problems in the real world). The antidote to this dystopia, and a key aspect of what the future holds, relies on our ability to educate citizens to embrace critical thinking.

7. Sovereignty and shifting power dynamics

In the workshops held in Europe, we heard concerns about a blurring of frontiers between governments and private corporations (for example, a few participants speculated about a future in which the largest tech companies hold seats on the UN Security Council). From US-based participants, we heard more concerns about a trend toward digital sovereignty, the security issues companies face in addressing increasingly divergent regulatory requirements around the world, and lack of a practical human rights framework for determining compliance trade-offs. Most agreed that the public sector will play an important role as both buyer and investor in technology and in developing guardrails in how cybersecurity plays out.

Planning for future cybersecurity risks

It is imperative for security practitioners to take a holistic view on the advancement of digital technologies to stay ahead of the curve. As per the Global Cybersecurity Outlook Report, a varied range of new technologies is being adopted by organizations, significantly raising the complexity of securing the digital ecosystem and widening the attack surface for malicious actors to exploit. It is therefore paramount to monitor how these technologies evolve, together with their social, economic and political contexts to make informed business decisions on organizational resilience.

The World Economic Forum, in collaboration with the Center for Long-Term Cybersecurity (CLTC), is running the Cybersecurity Futures 2030 initiative. It is a foresight-focused scenario-planning exercise to inform cybersecurity strategic plans and enable practitioners to understand the impact and prepare for the future of digital security. (Courtesy weforum.com)

About The Author

Akshay Joshi is the Head of Industry and Partnerships, Centre for Cybersecurity, World Economic Forum.