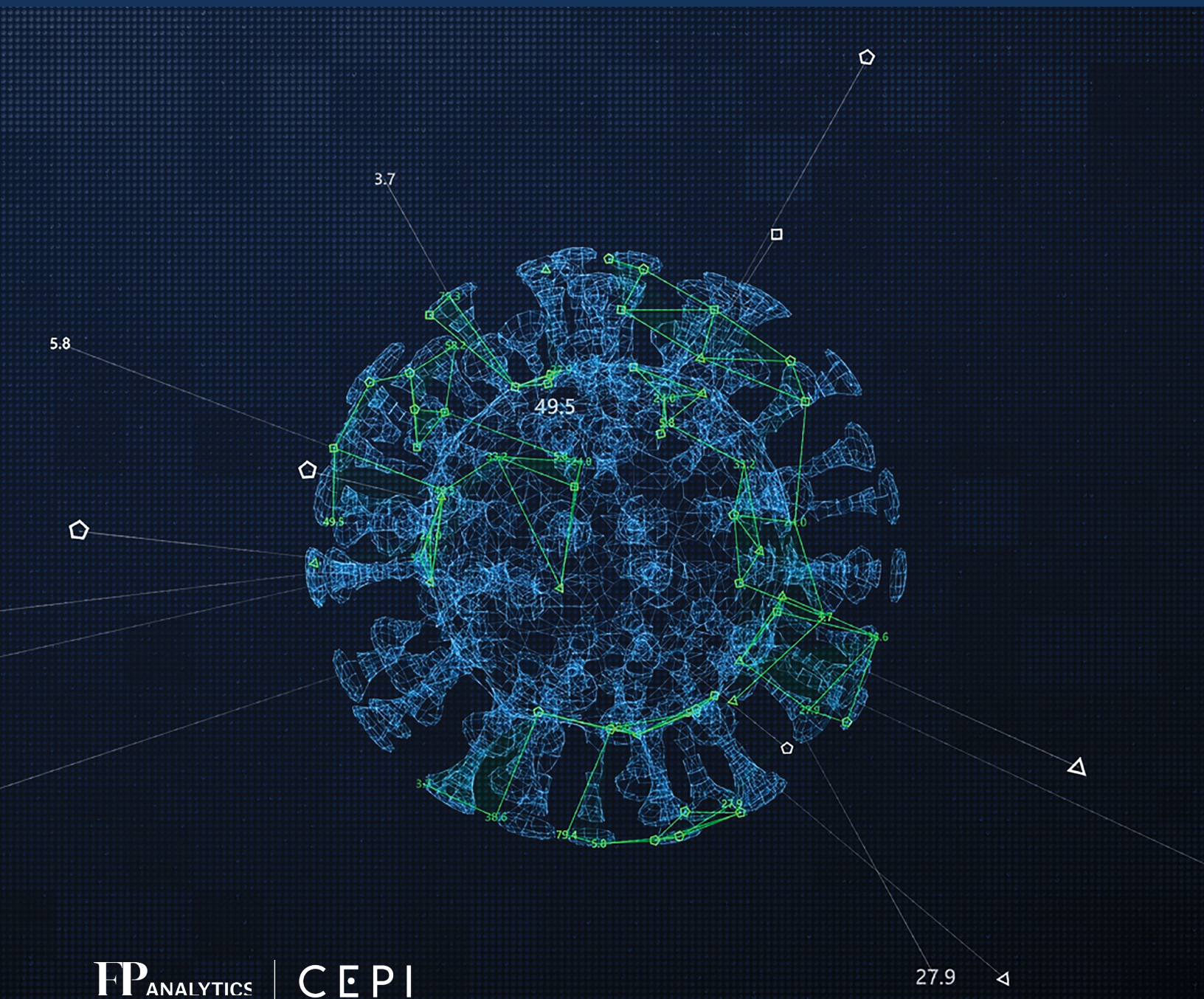
PUBLISHED APRIL 2024

Fighting 'Smart' Pandemics

Mitigating Risks and Harnessing the Potential of AI for Biosecurity



FP ANALYTICS | CEPI

A synthesis report produced by **FP Analytics**, with support from **CEPI**

Four years after the pandemic began, COVID-19 has killed an estimated seven million people worldwide and cost the global economy over $12 trillion. As the global community takes stock of lessons learned, there is broad consensus that far more political and economic investment is needed to improve pandemic preparedness and strengthen global health security. There is also growing recognition that emerging technologies present both extraordinary opportunities and evolving risks for this work. Recent advances in the application of artificial intelligence (AI) to biotechnology could help ensure that the next pandemic kills far fewer people—or that it kills vastly more.

AI has the potential to revolutionize the detection, attribution, prevention, and treatment of, and response to, epidemic and pandemic potential pathogens. At the same time, international governance and regulatory frameworks have not kept pace with technological developments, even as the number of labs studying high-consequences pathogens increases. Absent responsible stewardship and development, novel biotechnologies combined with AI systems could facilitate the creation and release of dangerous new pathogens, with the potential to unleash cascading consequences for global health, trade, economic development, and security.

Each year, FP Analytics (FPA) invites practitioners, experts, and thought leaders to participate in interactive, scenario-based simulations that foster dialogue and seek innovative solutions to pressing global issues. In February 2024, FPA partnered with the Coalition for Epidemic Preparedness Innovations (CEPI) and the Munich Security Conference (MSC) to produce a simulation, "Fighting 'Smart' Pandemics." The simulation built upon a multistakeholder roundtable discussion that FPA and CEPI co-hosted on the sidelines of the 2023 UN General Assembly, which highlighted the intersection of AI and biosecurity as a key priority area warranting deeper and sustained engagement from global leaders. CEPI, alongside the International Pandemic Preparedness Secretariat, has led a "100 Days Mission" to enable the design, testing, and development of pandemic countermeasures within 100 days of an epidemic or pandemic threat's emergence, a goal supported by the G7 but not yet realized.

The simulation, held alongside the MSC, brought together 24 senior leaders from across the security, health, and tech sectors, including industry, academia, governments, think tanks, non-governmental organizations (NGOs), and multilateral institutions. Their task was to consider a hypothetical scenario in which an AI-engineered pathogen spreads rapidly around the world, with the goal of identifying opportunities to reduce global biosecurity vulnerabilities. The insights gleaned from this diverse and experienced group, supplemented by FPA's independent research, highlight the urgent need for coordinated cross-sectoral action, investment, regulation, and collaboration to strengthen global biosafety, biosecurity, and pandemic preparedness. This synthesis report distills key takeaways from the dynamic and immersive simulation, focused on mitigating the risks and harnessing the potential of AI and biosecurity.

KEY TAKEAWAYS

- **Harness AI's life-saving applications across sectors.** Cross-sectoral partnerships are critical to realize the potential of AI-powered biotech in disease detection, surveillance, and attribution; medical countermeasure design, testing, and manufacturing; and global health emergency response. The private tech sector can play a leading role in sharing expertise and research into AI and other emerging technologies, particularly into their capabilities, vulnerabilities, and pitfalls.

- **Strengthen national and global governance of emerging technology with potential for misuse.** States, multilateral institutions, and the private sector need to collaborate transparently and consistently to safeguard

against the likeliest sources of manmade pandemics—including generative AI, synthetic genetic material, and benchtop synthesizers—more effectively.

- **Combat mis- and disinformation.** AI can both power and be the subject of mis- and disinformation that deceives and confuses the public. Effective pandemic response will require coordination on messaging among the government, media, and community-based organizations to limit the impact of mis- and disinformation campaigns on public awareness and trust.

- **Develop and implement research- and performance-based biosafety and biosecurity standards.** The increasing number of laboratories performing high-consequence biological research demands the development of research-based biosafety and biosecurity norms and standards that build competence and confidence in vital scientific discovery. Performance-based approaches could help inform research funding and publication decisions, recognize facilities with strong safety and security track records, and identify suitable facilities for emergency research.

- **Democratize access to pandemic preparedness supplies.** The development, manufacture, distribution, storage, and ownership of biotechnologies, medical countermeasures, and medical equipment need to be safely and securely democratized to accelerate global health equity. Strengthening and localizing medical supply chains, licensing generic medicines for manufacture, and supporting research and development in the global south will ensure that these resources can be mobilized rapidly by communities in need. The development of global health commons platforms—such as a vaccine library—accessible to trusted stakeholders is one promising approach that could be paired with other strategies and mechanisms.

- **Invest in biodefense.** Biodefense historically has been underprioritized in security budgets, policy agendas, and defense strategy. Investments in biosafety and biosecurity need to be sustained in between public health emergencies to bolster recent gains in preparedness and resilience and to break the cycle of neglect and panic associated with epidemics and pandemics.

Summary of the Game and Participant Insights

FPA's fictional scenario was set in December 2025. Participants were paired up and assigned to roles whose interests and perspectives they were expected to represent throughout the simulation's two "moves." Roles included the European Union (E.U.), the World Health Organization (WHO), the World Bank, the UN Office for Disarmament Affairs (UNODA), the Africa Centres for Disease Control (Africa CDC), a fictional Private Sector Health and Pharmaceutical Coalition, a fictional Responsible Use of AI Coalition, and the governments of Brazil, China, India, Kenya, South Africa, and the United States (U.S.).

Move 1: Detection and Rapid Response

December 2025

In the first move, media outlets reported the emergence of a novel respiratory illness in Asia associated with encephalitis and high mortality. The disease was from the paramyxovirus family, which is endemic to the region and typically of zoonotic origin. However, unexpected mutation patterns prompted some scientists to suggest it may have been genetically engineered. Within weeks, the virus reached Europe and Africa, overwhelmed hospitals, killed a fifth of those infected, and created dire shortages of personal protective equipment (PPE), medical supplies, and test reagents.

In response, global data sharing began in earnest, and a fictional, newly formed international NGO—the "Global Vaccine Library Consortium" (GVLC)—mobilized to address the crisis. The fictional GVLC leveraged AI to accelerate the design, development, testing, manufacture, and deployment of an effective vaccine worldwide as rapidly as possible. However, disinformation campaigns emerged on social media claiming that AI technologies were dangerous and could not be trusted. The theories proved especially popular in countries impacted by vaccine inequities during the COVID-19 pandemic.

PARTICIPANTS' RESPONSES AND ACTIONS

In response to Move 1, the teams role playing the Responsible Use of AI Coalition and the WHO collaborated to disseminate trustworthy, fact-based information across media platforms, including regarding the efficacy and safety of AI-enabled vaccines. Meanwhile, the priority for those role playing national governments and institutions in the global south was to ensure an adequate supply of vaccines, PPE, and other countermeasures. The team role playing theAfrica CDC noted its lack of respirators, and the team role playing India noted inadequate vaccine supplies, with both seeking to meet their needs through regional manufacturing and partnerships to bolster supply chains. By contrast, the team role playing China emphasized its investment in pandemic preparedness and vaccine development but contended that its vaccines faced unwarranted distrust during the COVID-19 pandemic, impacting its ability to collaborate beyond its borders. More generally, participants noted concerns over vaccine misinformation and broader public distrust of public health guidance and authorities as key challenges to ensuring an effective response.

A 100-day timeline for design, manufacture, and deployment of vaccine countermeasures was proposed to facilitate rapid pandemic response and containment. Such an approach could save millions of lives in a pandemic situation but would require proactive investments to ensure that the global community is equipped with the necessary capabilities to move fast once the next threat emerges. However, the team role playing the E.U. noted the need for global manufacturing capabilities to ensure that sufficient doses of a safe and affordable vaccine would be available to the most vulnerable communities. In response to these concerns and calls for greater distribution of vaccines in under-resourced countries, the team role playing a fictional Private Sector Health and Pharmaceutical Coalition highlighted the complexities of global vaccine distribution, noting the need for cross-sectoral cooperation and coordination. The Private Sector Health and Pharmaceutical Coalition called on governments to work with them proactively to meet the needs of affected populations.

Move 2: Attribution and Prevention

July 2026

Move 2 established that by July 2026, the global community had designed and manufactured a safe and effective vaccine for the new disease. As a result, vaccination rates increased, the pandemic slowed, and the immediate crisis eased. However, an anarchist terror group soon claimed responsibility for creating and releasing the virus. Intelligence agencies determined that the group had recruited disgruntled scientists, stolen equipment and materials from a high-security laboratory, and leveraged AI tools to design and produce the virus. In response, the WHO convened an International Biosecurity Summit to discuss emerging risks and necessary guardrails.

PARTICIPANTS' RESPONSES

Information revealed in Move 2 regarding the origin of the virus shifted participant responses and priorities toward security issues, and to the question of how defense and health resilience interact. Several participants, including the team role playing China, conceptualized the virus as a weapon of mass destruction and noted UNODA's significant role in controlling and responding to the use of such weapons. In response, the team role playing UNODA triggered the Secretary-General's Mechanism for investigating bioweapons allegations but noted the challenges of attribution resulting from the pathogen's multinational sourcing and development. This prompted the teams role playing the U.S. and E.U. to call for stronger security standards in labs and coordinated global approaches to identify and prevent bioweapons development. Several participants noted shortcomings in the Biological Weapons Convention, arguing that it was easily stymied by intransigent states.

In addition to discussing attribution and response to the immediate crisis, participants debated how best to avoid misuse of this technology moving forward while maintaining and promoting the beneficial uses of AI. The team role playing the fictional Responsible Use of AI Coalition, for example, noted that despite its use in the development of the virus, AI was also crucial to saving lives through rapid vaccine development. The team argued that the tech industry has an obligation to self-regulate given that it is best positioned to understand these technologies' potential misuses, but noted that punitive regulation could stifle life-saving innovation. The team also acknowledged the need for greater engagement and coordination with the public sector on guidelines and guardrails applicable to AI in health care and biosecurity.

Participants role playing both the E.U. and China teams noted that safety requires not only regulation but also strong surveillance, detection, response, and accountability systems. The team role playing the WHO called for regulation that is proactive and preventive, instead of solely responsive. Such systems and regulations will be important globally but could make an especially significant difference to health security in lower-income countries. As the team role playing Africa CDC emphasized, the global south has suffered from the impacts of global health inequity and insecurity—in this case suffering from a virus it did not produce, made with technology it did not develop.

Reflections on Risks and Opportunities

Following the simulation, participants were invited to step outside of their assigned roles and reflect on the simulation's implications for real-world health security based on their expertise and experience. These insights, alongside independent research conducted by FPA to design the simulation, provide context and depth to the exercise itself and generate key takeaways relevant to cross-sectoral stakeholders in strengthening global health security.

Unregulated access to DNA synthesis capabilities could threaten global health security

One key takeaway from the simulation is the recognition that AI technologies alone cannot produce a pathogen without a physical synthesis process. Thus, safeguards are essential at the point of synthesis: the point where digital information becomes a physical product. Participants described screening DNA synthesis orders as an urgent, essential method of reducing potential misuse of AI technology.

The price of bespoke, mail-order DNA sequences has plummeted in recent decades, and it is now possible to order strands of DNA that are long enough to stitch together to create a dangerous pathogen. While many synthesis companies coordinate across the industry to screen orders for dangerous sequences and to ascertain valid professional or academic use, such screening is legally optional and non-standardized, and it can be evaded by ordering from less-scrupulous vendors and competitors. Furthermore, "benchtop" synthesizers (so named for their ability to fit on a lab bench) now allow users to evade third-party scrutiny by "printing" genetic material themselves. In the absence of adequate governance, this technology could lower the barrier to creating dangerous pathogens through gene synthesis.

The potential impact of increased access to these technologies is well documented and increasingly clear. In 2016, a small team of virologists at the University of Alberta proved that due to advances in genetic engineering, one of the greatest public health achievements in world history could be undone. Using mail-order DNA fragments, the group successfully synthesized horsepox—a close relative of smallpox—in six months, with a budget of $100,000. The effort "did not require exceptional biochemical knowledge or skills," according to the WHO, and there is "no question" that the same techniques could also be used to recreate the highly contagious and deadly smallpox, which was officially eradicated in 1980. Mandatory screening related to the distribution and purchase of synthetic DNA and equipment, including benchtop synthesizers, could therefore mitigate the malicious engineering and weaponization of pathogens, which is critical to safeguarding public health and strengthening global biosecurity.

Generative AI models could increase the risk of biological misuse

The health security risks presented by generative AI depend on the particular technology in question. "Generative AI" is an umbrella term describing a wide range of AI

applications, including large-language models (LLMs) and bio design tools (BDTs). The best known LLMs are publicly available, general-purpose AI chatbots like Chat GPT. Mitigating risks presented by generative AI will require differentiated approaches to BDTs, compared to AI chatbots. Preliminary research by Open AI and the RAND Corporation suggests that these chatbots offer only limited practical and scientific guidance toward the planning and execution of biological attacks. For example, in the RAND study, an LLM suggested virus delivery methods and research cover stories, and discussed practical aspects of obtaining materials and projected death tolls. However, to date, chatbot LLMs have not generated explicit instructions for creating biological weapons, and much of the information they provide is already widely available elsewhere on the internet. Chatbots summarize complex science and collate information from far-flung sources, but they generally do not provide motivated actors with previously inaccessible information.

The more serious long-term risk from AI comes from BDTs, which are often built on LLMs trained on extensive databases of amino acid sequences. Instead of generating natural-sounding written language, these LLMs generate genetic sequences that are likely to produce desired properties. This capability makes them extremely useful to beneficial life sciences research—for example, by reducing the number of sequences researchers must test before finding one that behaves in a desired way. Unlike general-purpose chatbots, the predictions provided by BDTs constitute genuinely novel scientific insights, which can be used for good or lead to harm either accidentally or maliciously. Currently, most BDTs are either not publicly available or difficult to use without deep knowledge of biology, computer programming, or both. Still, combined with increasingly affordable and user-friendly DNA synthesis options, this capability could present grave new biosecurity risks, which cross-sectoral cooperation and regulation can help mitigate.

Safeguards are needed to prevent AI bias from undermining health equity

Misuse of AI poses additional risks to health equity beyond its potential to fabricate or replicate dangerous pathogens. An AI system is only as smart as the data on which it is trained, and that data is often biased in ways that reflect or exacerbate existing inequalities. In a health care context, for example, the most detailed and complete data available is often drawn from wealthy western countries, which are not representative of the world's genetic makeup, climate, or socioeconomic health factors. Furthermore, those who train AI may label data or design model architecture in ways that reflect their own biases. Safe and effective AI-driven vaccines and other countermeasures need to be developed and distributed in a way that is open, transparent, accountable, and—as simulation participants advocated—balances human rights with tech-driven innovation. This goal will require the closure of data gaps around the world, and the buy-in and cooperation of underserved, under-resourced communities that are among the most vulnerable in pandemics and other public health or humanitarian catastrophes.

AI-driven mis- and disinformation could inhibit public health responses

AI-powered deception can spread false information and undermine trust in public health authorities, slowing the speed and effectiveness of society's response to health emergencies. As a result, effective response to any pandemic will require clear, trustworthy messaging through which to share resources and information. Simulation participants noted the importance of strengthening public trust in government and health institutions, bolstering local, independent media, and engaging with trust and safety teams on social media and other tech platforms to combat the spread of false information. Crucially, such work will also enable health authorities to leverage these platforms to spread reliable information instead.

Lab safety protocols need to keep pace with the rapid expansion of high-consequence research and research facilities

Beyond the possibility of malicious misuse, global health security could be threatened by the accidental release of dangerous pathogens being studied in research laboratories. A surge in legitimate research involving high-consequence pathogens offers promising applications and societal benefits but also increases the risk that these pathogens could be accidentally released. A 2023 report noted "several trends that raise biosafety and biosecurity concerns," including a boom in the construction of BSL4 and BSL3+ labs in places with weak governance, stability, or oversight; limited safety standards; and limited research into which safety measures are actually effective. Accidents have likely caused pandemics before: the 1977 flu pandemic, for example, likely resulted from either a lab leak or a botched vaccine trial and killed approximately 700,000 people worldwide. Strengthening and standardizing lab safety protocols, including through the development and implementation of risk- and performance-based standards, is therefore crucial to saving lives from both malicious and accidental pathogen leaks.

AI can be an asset for biodefense and global health security

While AI tools have the potential to be misused for malicious reasons, they are also indispensable in the effort to stay one step ahead of the next pandemic or malicious actor. Coupled with bio-surveillance techniques such as sampling wastewater or air quality, AI can be used to detect the presence of novel pathogens, and track and forecast their spread before tests in humans are available. This can help policymakers target interventions to the right populations at the right time, which is particularly important in low-resource settings. Deployed alongside genomic sequencing, AI can also predict how pathogens may evolve, including when and where they might acquire resistance to antimicrobial treatment. If resistance does develop, AI systems can enable rapid detection and the design of new antibiotics that overcome resistance.

AI is also useful for the attribution of genetic engineering efforts, a necessary step in deterring and penalizing the use of bioweapons. For example, a genetic engineer's chosen approaches and techniques create a "methodological signature" that can, with AI, help trace a pathogen back to its likely designer. A 2018 study trained an AI network on a dataset with 42,364 engineered DNA sequences from 2,230 labs and found that it could identify the lab source 48 percent of the time and place it in the top 10 predicted labs 70 percent of the time. Such capabilities could enable monitoring, detection of, and rapid response to biological attacks, and thereby help to deter future incidents.

AI is also useful for developing countermeasures for yet-to-be-discovered viruses (referred to as "Disease X" threats in public health discourse), giving vaccine researchers, developers, and distributers a crucial head start in addressing the next pandemic. Only 26 viral families have historically been implicated in human disease, and applying AI to massive virus databases allows researchers to rank which families pose the greatest pandemic threat based on known risk factors. From there, scientists can again use AI to design vaccine prototypes for priority families, which could be collated in global commons platforms such as vaccine libraries and quickly adapted to novel viruses as they arise. Similar approaches can hasten development of therapeutics and diagnostics, allowing rapid testing and treatment in a pandemic scenario.

For these reasons, applying AI is necessary to achieving the 100 Days Mission—and, in turn, to saving untold thousands of lives. COVID-19 killed at least 5,000 people per day—likely an undercount—from June 2020 to May 2022 and cost the global economy trillions of dollars per year. The next pandemic could be far more lethal, and the burden is likely to again fall hardest on disadvantaged, resource-scarce, and vulnerable communities, despite recent strides to reduce health inequities. Developing life-saving countermeasures as quickly as possible is a global health priority for stakeholders across all sectors, making AI a powerful asset for biodefense.

Looking Ahead

In an increasingly connected and tech-enabled world, preventing and responding to borderless health crises is a complex challenge. To meet it, forward-thinking leaders will need to anticipate and incorporate the power of emerging technology, with necessary guardrails identified and in place. Research-based crisis simulations can help leaders grapple with this technology's complex, unprecedented, and far-reaching implications, identify critical vulnerabilities, and chart-out and pursue viable solutions.

The 2024 "Smart Pandemics" simulation encouraged reflection and discussion of the risks and opportunities that AI presents to biosecurity. Participants noted the need to balance innovation with regulation, and security with equity; to collaborate across borders, sectors, and disciplines; and to ensure that governance keeps pace with AI's capabilities to avoid empowering bad actors.

Efforts are underway at both national and international levels toward these ends. In December 2021, member states of the WHO agreed to draft and negotiate a global treaty to strengthen pandemic prevention, preparedness, and response. As of April 2024, an Intergovernmental Negotiating Body has developed multiple negotiating texts with a final draft text to be discussed at the May 2024 World Health Assembly. The current draft focuses on equitable access and benefit sharing, capacity-building for research, manufacturing and pandemic response, health system resilience, global health security collaboration, and ensuring sustained and sufficient political and financial investment within and among nations. Additionally, in March 2024, the UN General Assembly adopted a landmark resolution (78/L.49) on artificial intelligence that includes efforts to address AI biosafety and biosecurity risks.

Similar investments have already borne fruit in Africa. Thanks in part to funding from the E.U., the Africa Center for Epidemic Resilience in Dakar opened in January 2024 and was certified by the Africa CDC as a Center of Excellence in Biosafety and Biosecurity for the West Africa region. The Africa CDC is also spearheading a Biosafety and Biosecurity Initiative to help protect Africans against the release of harmful biological agents, as well as an ambitious Digital Transformation Strategy to strengthen public health systems across the continent. Uganda has agreed to lead the execution of the WHO's Global guidance framework for the responsible use of the life sciences in the East Africa region. In March 2024, the UN Food and Agriculture Organization hosted a workshop on Laboratory Biosafety and Biosecurity in Accra, Ghana, while the Africa CDC held a convening in Addis Ababa, Ethiopia, to review and accelerate progress toward health security on the continent.

The U.S. Congress is negotiating a reauthorization of the Pandemic and All Hazards Preparedness and Response Act, which aims to bolster global biodefense in a wide range of ways. For example, the Senate version of the proposed reauthorization includes investments in innovation toward "Disease X" countermeasures; strengthened public health communication; support for at-risk populations; updated rules for the possession of dangerous pathogens; a no-fault reporting system for lab accidents or safety incidents; and a study on AI threats to health security. However, although the legislation calls for updated federal guidance on screening gene synthesis orders, such guidance would remain voluntary. The U.S. accounts for 40 percent of the global synthetic biology market, so producers in other countries and regions would have significant incentive to comply with American screening regulations if enacted.

The 2024 "Smart Pandemics" simulation reaffirmed that the global community remains unprepared for both conventional and tech-enabled public health and biosecurity crises. While the simulation uncovered promising ideas to begin closing the preparedness gap, implementation will require time, money, expertise, and multistakeholder cooperation before an emergency occurs, amid competition for resources with more immediate priorities. To avoid catastrophe, leaders around the world will need the prescience, conviction, courage, and resolve to avoid the potential damage of emerging technologies and seize the opportunities that they hold for global health and security.

By Andrew Doris (Senior Policy and Research Analyst), Isabel Schmidt (Senior Policy Analyst and Research Manager), and Dr. Mayesha Alam (Vice President of Research), with direction from Allison Carlson (Executive Vice President of FP Analytics and Events).

This synthesis report was produced by FP Analytics, the independent research division of The FP Group, with support from The Coalition for Epidemic Preparedness Innovations (CEPI). FP Analytics retained control of the research direction and findings. Foreign Policy's editorial team was not involved in the creation of this content.

FP ANALYTICS | CEPI