JANNE E. NOLAN CENTER
COUNCIL ON STRATEGIC RISKS

BRIEFER

No. 54 | September 14, 2023

THE CYBER-BIOSECURITY NEXUS: KEY RISKS AND RECOMMENDATIONS FOR THE UNITED STATES

By Abi Olvera

Edited by John Moulton and Christopher East

The views expressed in this briefer belong solely to the author and do not represent those of the U.S. government.

Whether to deny service, steal intellectual property, or propagate disinformation, countries such as Russia and North Korea have shown their willingness and ability to conduct malicious cyber activities through times of crisis and relative repose. Attacks on critical infrastructure, biotechnology enterprises, and medical research institutions highlight the need to prioritize prevention, improve detection, and scale national response mechanisms amidst the growing sophistication of malicious actors at this nexus. Such issues, which are increasingly referred to as "cyber-biosecurity" risks, have become a new toolset in the growing sub-threshold arsenals of those that oppose the rules-based international order.

This briefer provides an overview of the trends and critical risks at the nexus of cybersecurity and biosecurity.[1] It then offers high-level recommendations for addressing these risks.

THREAT DRIVERS

Risks in this space are rising due to several trends that this section will explain in brief: rapid advances, democratization of synthetic biology, global proliferation of high-containment facilities, diversification of attack vectors, and diversification of biological targets.

1 Author's Note: Risks associated with machine learning risks are intentionally omitted as they will be covered in a forthcoming briefer dedicated to AI-Biosecurity.

RAPID ADVANCES IN AUTOMATION

The convergence of robotics, machine learning, cloud computing, and synthetic biology has paved the way for positive advances in automated approaches to biology[2] while simultaneously creating new cyber-biosecurity vulnerabilities.[3] At the same time, distributed manufacturing has increased the risk of unauthorized remote access to sensitive biological data, processes, and products.[4] Automation has quickly become the norm among research and production as well, with cell programming foundry giant Ginkgo signing a $10 million deal with a robotic cloud lab in 2017, expected to double Gingko's monthly foundry output.[5] Automation in production workflows, paperwork, and quality testing enabled rapid conversion of existing vaccine facilities to swiftly manufacture billions of mRNA vaccine doses at the unprecedented pace and scale needed to combat COVID-19.[6]

DEMOCRATIZATION OF SYNTHETIC BIOLOGY

Innovation in the life sciences and biotechnology sectors brings considerable benefit but also increased risks. Synthetic biology is easier, cheaper, and more ubiquitous than ever before. The de novo synthesis of dangerous pathogens has been made easier through technological advances,[7] with developments outpacing regulation.[8]

Several trends are at play. More people have the access and skills to perform high-risk research[9] due in part to the price of DNA sequencing and synthesis falling significantly over the last ten years.[10] Additionally, experiments can now

---

2 Richardson, Lauren C., Nancy D. Connell, Stephen M. Lewis, Eleonore Pauwels, and Randy S. Murch. "Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape."

3 Murch, Randall S., William K. So, Wallace G. Buchholz, Sanjay Raman, and Jean Peccoud. "Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy."

4 "Increase Vigilance Against Cyberattacks." Nature Biotechnology 40, no. 8 (August 2022): 1155–1155.

5 Ginkgo Bioworks. "Ginkgo Bioworks Taps Transcriptic's Robotics Software to Further Accelerate Automation in Organism Design." October 3, 2017.

6 Siemens Thailand. "Speeding up Covid-19 vaccine production setup with automation," n.d.

7 Esvelt, Kevin M. "Inoculating Science against Potential Pandemics and Information Hazards." Edited by Carolyn B. Coyne. PLOS Pathogens 14, no. 10 (October 4, 2018).

8 Sandberg, Anders, and Cassidy Nelson. "Who Should We Fear More: Biohackers, Disgruntled Postdocs, or Bad Governments? A Simple Risk Chain Model of Biorisk." Health Security 18, no. 3 (June 1, 2020): 155–63.

9 Esvelt, Kevin M. "Inoculating Science against Potential Pandemics and Information Hazards." Edited by Carolyn B. Coyne. PLOS Pathogens 14, no. 10 (October 4, 2018).

10 Genome.gov. "The Cost of Sequencing a Human Genome," November 1, 2021; Sandberg, Anders, and Cassidy Nelson. "Who Should We Fear More: Biohackers, Disgruntled Postdocs, or Bad Governments? A Simple Risk Chain Model of Biorisk." Health Security 18, no. 3 (June 1, 2020): 155–63.

be performed remotely through cloud laboratories,[11] which presents a concerning trajectory towards 'de-skilling' research by reducing some of the knowledge requirements for conducting sophisticated research protocols.[12] Remote experimentation can allow malicious actors to bypass ethical constraints present in traditional academic laboratories.

GLOBAL PROLIFERATION OF HIGH-CONTAINMENT FACILITIES

The number of high biosafety level containment facilities worldwide has grown significantly in the past three decades, with nearly such sixty facilities now in operation.[13] This increase is driven by the demand for high-risk research, which requires strict adherence to established procedures and adequate supervision to ensure it is safely conducted.[14] Seventy-five percent of the labs worldwide are located in urban centers, while according to the Nuclear Threat Initiative's Global Health Security Index,[15] only a quarter of the countries with biosafety level 4 (BSL-4) labs score highly on best practice indicators for biosafety and biosecurity.[16] Labs that use cloud-based biosafety systems could present a particularly accessible means for malicious actors to exploit.[17] The rapid spread of laboratories, especially in countries that score low on biosecurity best practice indicators, could generate numerous vulnerable targets where high-risk research could potentially be stolen, manipulated, or released.

DIVERSIFICATION OF ATTACK VECTORS

Cyber-biosecurity attack vectors are increasingly apparent in public records of events. For example, in 2017 a team of researchers embedded malware into DNA and successfully hacked a computer attempting to analyze genetic data.[18] While the malware test was conducted in a controlled and artificially vulnerable environment, some researchers worry

---

11 In 2017, a review of 1628 scientific papers found that 86-89% reported one or more methods that could be conducted in a cloud laboratory - Groth, Paul, and Jessica Cox. "Indicators for the Use of Robotic Labs in Basic Biomedical Research: A Literature Analysis." PeerJ 5 (November 8, 2017): e3997.

12 World Health Organization. "Emerging technologies and dual-use concerns: a horizon scan for global public health." Emerging technologies and dual-use concerns: a horizon scan for global public health, October 22, 2021.

13 George Mason University Schar School of Policy and Government. "A New Interactive Map Reveals Where the Deadliest Germs Are Studied," July 8, 2021.

14 Homeland Security News Wire. "Improving Safety in Labs Dealing with Lethal Viruses," October 29, 2021; C5 Capital. "The Nexus Between Cybersecurity and Biosecurity White Paper," May 13, 2020.

15 Joseph Rodgers, Filippa Lentzos, Gregory D. Koblentz, Minh Ly. "How to make sure the labs researching the most dangerous pathogens are safe and secure." Bulletin of the Atomic Scientists, July 2, 2021.

16 Ibid.

17 Crawford, Elizabeth, Adam Bobrow, Landy Sun, Sridevi Joshi, Viji Vijayan, Stuart Blacksell, Gautham Venugopalan, and Nicole Tensmeyer. "Cyberbiosecurity in High-Containment Laboratories." Frontiers in Bioengineering and Biotechnology 11 (July 25, 2023).

18 Regalado, Antonio. "Scientists Hack a Computer Using DNA." MIT Technology Review, August 10, 2017.

that hackers could now conduct malware attacks through DNA. The flaw that enabled the hack still persists: computers read extra code, in this case hidden in genetic data, as legitimate commands (also known as a "buffer overflow attack").[19]

Cyber attacks on critical infrastructure are now proven pathways for impacting public health. In 2021, attackers manipulated the chemical levels of water treatment facilities in Florida and California which could have posed a significant risk to public health.[20] Additionally, the widespread use of networked devices, such as lab robots and climate control systems, make medical providers highly vulnerable to cyber breaches, theft, and unauthorized access. Researchers have found multiple theoretical cyber vulnerabilities via networked equipment that could, for example, target microbial forensics efforts and thus hamper the government's ability to distinguish naturally occurring events from deliberate events.[21] A U.S.-based hacking group installed malware into a Texas hospital's HVAC system and dozens of computers with patient records.[22] HVAC systems appear to currently be potential vectors of attacks, in particular, via ransomware[23] and potential power surges.[24]

DIVERSIFICATION OF BIOLOGICAL TARGETS

Biosecurity experts have long tracked threats across many sectors and nodes. Similarly, cyber vulnerabilities appear to be expanding to more diverse biosecurity-relevant targets. Food production has become highly technologized, with farmers utilizing remote sensors, automation, edge computing, and heavy computerized equipment to boost efficiency, which has increased the vulnerability of agricultural systems to cybersecurity threats.[25] Cyber attacks on agricultural production rose 607%[26] from 2019 to 2020, resulting in supply chain disruptions, ransomware incidents, and intellectual property theft. A cyberattack on a Minnesota agricultural cooperative disrupted the livestock feed order and an Iowa farming co-op was hit by ransomware which disrupted the networks responsible for the feeding schedules of chickens, hogs, and cattle.[27] In 2021, JBS, the largest meat processing company in the world, paid out an $11 million ransom in response to an attack that shut down plants, increased beef prices, and led to Food and Drug Administration (FDA) intervention to encourage production at other companies.

---

19 Reed, J. Craig, and Nicolas Dunaway. "Cyberbiosecurity Implications for the Laboratory of the Future." Frontiers in Bioengineering and Biotechnology, August 21, 2019.

20 Magill, Jim. "U.S. Water Supply System Being Targeted By Cybercriminals." Forbes, July 27, 2021.

21 Reed, J. Craig, and Nicolas Dunaway. "Cyberbiosecurity Implications for the Laboratory of the Future." Frontiers in Bioengineering and Biotechnology, August 21, 2019.

22 Poulsen, Kevin. "Leader of Hacker Gang Sentenced to 9 Years For Hospital Malware." Wired, March 18, 2011.

23 Alder, Steve. "HVAC Vendor Allegedly Hacked: Access Gained to Hospital Systems." HIPAA Journal, August 23, 2021.

24 Yang, Elvina. "Smart HVAC systems vulnerable to being controlled by hackers through cyber attacks." ASMag, October 27, 2019.

25 Rundle, James. "Food Producers Band Together in Face of Cyber Threats." Wall Street Journal, June 15, 2023.

26 Creasey, Simon. "Tech leaves food industry more exposed to cybersecurity threat." Just Food, March 14, 2023.

27 Kouloufakos, Triantafyllos. "Digital Agriculture—A Gap in Critical Infrastructure Protection." Council on Foreign Relations, December 15, 2022.

Experts at the University of Minnesota's Food Protection and Defense Institute noted that cyber incidents could also lead to tainted food, injury or death of plant workers, and more simultaneous plant shutdowns than those seen during the COVID-19 pandemic.[28] Some experts and officials have raised concerns that while precision agriculture technologies like GPS sensors that guide tractors to spray optimized fertilizer mixes and internet-connected computers precisely controlling temperature and humidity in enclosed commercial chicken houses enable efficient large-scale farming, they also provide vulnerabilities that hackers could exploit to sabotage crops by poisoning fields or quickly killing tens of thousands of chickens by disrupting environmental control systems.[29]

CRITICAL VULNERABILITIES IN THE UNITED STATES

The life sciences and biotechnology sectors, given their highly sensitive R&D programs, distributed manufacturing systems, numerous externally-facing collaborators, and in some cases relatively weak security, make them among the sectors most susceptible to cyber attacks.[30] Healthcare cyber threats account for 24.5% of all hacks, with each breach costing an average of $5 million.[31] A March 2021 study found that almost 92% of the pharmaceutical organizations surveyed suffered at least one database exposure.[32] Ransomware and Denial of Service (DDoS) attacks are both lucrative and disruptive to patient care and research.

Unfortunately, events during the COVID-19 pandemic showed the various ways that nefarious actors can target the capabilities most needed for responding to significant biological events. Attacks originating from Russia disrupted critical supply chains during the height of the COVID-19 pandemic response. For example, global firm Miltenyi Biotec suffered a two-week outage in November 2020 while sequencing COVID samples.[33] The same month Americold, the largest cold storage operator in the United States, was in talks to provide storage for the distribution of COVID-19 vaccines when it suffered a cyber attack.[34] The 2017 Russia-linked NotPetya malware attack on Merck's central computer systems led to the company losing control of over 30,000 computers and the encryption of critical data across sales, research, and manufacturing. Merck also suffered a two-week outage of computers used in the production of Hepatitis B and Human Papilloma Virus vaccines, resulting in global supply shortages.[35]

---

28 Starks, Tim. "The Food and Agriculture Industry Gets a New Center to Share Cybersecurity Information." Washington Post, May 24, 2023.

29 Geller, Eric. "The Dangerous Weak Link in the US Food Chain." Wired, April 6, 2023.

30 "Increase Vigilance Against Cyberattacks." Nature Biotechnology 40, no. 8 (August 2022): 1155–1155.

31 "Increase Vigilance Against Cyberattacks." Nature Biotechnology 40, no. 8 (August 2022): 1155–1155; Reed, J. Craig, and Nicolas Dunaway. "Cyberbiosecurity Implications for the Laboratory of the Future." Frontiers in Bioengineering and Biotechnology, August 21, 2019.

32 Venkateswaran, Vikram. "Cybersecurity Is a Top Priority for Pharmaceutical Organizations." ISACA, October 11, 2022.

33 "Increase Vigilance Against Cyberattacks." Nature Biotechnology 40, no. 8 (August 2022): 1155–1155.

34 Davis, Jessica. "Hackers Hit COVID-19 Biotech Firm, Cold Storage Giant with Cyberattacks." Health IT Security, November 18, 2020.

35 "Increase Vigilance Against Cyberattacks." Nature Biotechnology 40, no. 8 (August 2022): 1155–1155.

While these examples showcased relatively straightforward types of attacks such as ransomware, intellectual property theft, and distributed denial of service, several other types of vulnerabilities are already becoming apparent within the United States, as noted below.

MALICIOUS GENOMIC ENGINEERING

Known vulnerabilities in synthetic DNA sequencing continue unresolved. In November 2020, Israeli researchers published the discovery of an active vulnerability where a bioengineer could unknowingly order synthetic DNA that had been tampered with by malware on their computer.[36] The researcher's tampered DNA successfully bypassed screening software despite the obfuscated DNA encoding a toxic peptide. If the bioengineer had used the manipulated DNA in cell transformation experiments, the bioengineer would have unknowingly created harmful proteins. One can imagine attacks of this type against manufacturers of biologicals or similarly important ingredients that could endanger the public. Similarly, though it would require an actor with a high level of sophistication (at least with today's technologies), sophisticated cyber attacks on safety systems could include the manipulation of electronic genomic sequences to enhance the infectivity, drug resistance, or host range of microorganisms.

MISUSE OF BIOLOGICAL DATA

Citizens are increasingly at risk from cyber threats targeting medical and life sciences. The value of patient medical records on the black market is up to $1,000 per record, nearly ten times the market rate for credit card data and social security numbers. This lucrative market makes medical records a prime target for exploitation, enabling medical identity theft, financial fraud, and blackmail. Additionally, compromise to the integrity or availability of sample sets, such as large biobanks and legacy collections of biological samples, or one-of-a-kind data sets from specific outbreaks or time periods, could pose an irreplaceable loss to science and research.[37]

Capture and manipulation of genomic data is also a growing risk due to the proliferation of personalized medicine.[38] With the advent of CRISPR and other gene editing technologies, in the years ahead it will grow easier to create personalized, more lethal, or resistant versions of known pathogens. The large troves of private genetic data could be used for biological warfare or other nefarious purposes. Pathogen genomes are not just unprotected but are often actively required to be disseminated publicly by funder mandates. Methods for going from sequences to viable viruses are increasingly within the reach of many labs.

---

36 Rami Puzis, Dor Farbiash, Oleg Brodt, Yuval Elovici, and Dov Greenbaum. "Increased cyber-biosecurity for DNA synthesis." Nature Biotechnology, December 2020.

37 Crawford, Elizabeth, Adam Bobrow, Landy Sun, Sridevi Joshi, Viji Vijayan, Stuart Blacksell, Gautham Venugopalan, and Nicole Tensmeyer. "Cyberbiosecurity in High-Containment Laboratories." Frontiers in Bioengineering and Biotechnology 11 (July 25, 2023); Top Pharma and Life Sciences Threats White Paper, Illusive, n.d.

38 Richardson, Lauren C., Nancy D. Connell, Stephen M. Lewis, Eleonore Pauwels, and Randy S. Murch. "Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape." Frontiers in Bioengineering and Biotechnology 7 (June 6, 2019).

MEDICAL DEVICE INCURSIONS

The medical device industry still lags in defending against cyber attacks on life-critical equipment. Insulin pumps, pacemakers, and implantable cardioverter-defibrillators with wireless capabilities have been under media scrutiny since the 2010s for their potential for being hacked to deliver a fatal jolt to its wearer, of either volts of electricity or doses of insulin.[39] While security experts note that the medical equipment industry has taken proactive steps to address cybersecurity concerns,[40] getting security issues fixed is still an uphill battle. An insulin pump company issued a voluntary recall program in 2018 only after the development and demonstration of a pump hacking app by security researchers to FDA officials, despite the company being aware of the security issues for an extended period of time.[41]

RECOMMENDATIONS

In light of these growing threats, it's imperative that the United States reinforce the security of domestic biosecurity assets and foster international cooperation. By doing so, not only are U.S. interests protected, but insights are also gained into the evolution of global cyber-bio threats, bolstering preparedness and strategic response capabilities. Our key recommendations are:

GOVERNANCE AND LEGISLATION

1. The current governance framework on cyber-related risks associated with human and industrial genomic data in the United States is weak.[42] Current U.S. law does not recognize human genomic data as personally identifiable information. Industrial genomic data has limited safeguards under intellectual property law. Addressing genomic data cybersecurity will require stringent privacy laws and robust security measures, while still promoting responsible innovation and data sharing within the scientific community. As Dr. Mark Rothstein suggests, Congress should pass a comprehensive health privacy law that expands protection from disclosure of health data and strengthens health data privacy through measures like right to be forgotten laws, required de-identification and confidentiality protections, prohibiting insurance discrimination based on genetic data, and comprehensive federal privacy legislation modeled on the General Data Protection Regulation (GDPR) while expanding Health Insurance Portability and Accountability Act of 1996 (HIPAA) safeguards.[43]

---

39 Wadhwa, Tarun. "Yes, You Can Hack A Pacemaker (And Other Medical Devices Too)." Forbes, December 6, 2012.

40 Vaas, Lisa. "Doctors disabled wireless in Dick Cheney's pacemaker to thwart hacking." Sophos Naked Security, October 22, 2013.

41 Hay Newman, Lily. "These Hackers Made an App that Kills to Prove a Point." Wired, July 16, 2019.

42 Natasha E. Bajema, Diane DiEuliis, Charles Lutes, and Yong-Bee Lim, "The Digitization of Biology: Understanding the New Risks and Implications for Governance," National Defense University Center for the Study of Weapons of Mass Destruction, July 2018.

43 Rothstein, Mark. "Is Health Privacy Worth the Cost?" in Confidentiality, Privacy, and Data Protection in Biomedicine, ed. E.S. Dove (Routledge, forthcoming 2024).

Congress should also accelerate passing a National Data Security and Privacy Protection as well as a National Breach Notification law, as per the Cyberspace Solarium Commission's 2020 report recommendations.[44]

2. The government should also consider designating the bioeconomy and biotech sector as critical infrastructure to expand such entities' access to additional security funding and protection.[45] To avoid catastrophic disruptions, digital agriculture must be integrated into critical infrastructure protection.[46] Guidance helping farmers secure exploitable precision equipment and remote controls for livestock facilities, akin to Canada's 2021 cybersecurity assessment program for the agriculture sector,[47] can safeguard U.S. food supply.

3. Coordination between the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Health and Human Services (HHS) to tighten healthcare cybersecurity through industry analysis and workforce training is essential. It has been the subject of bipartisan legislation, but the bills have seen no activity since late 2022. Legislative fixes in this area would ensure CISA and HHS provide appropriate resources to prevent, detect, and respond to cyber incidents in the healthcare sector if enacted.

RAISING HIGH-RISK RESEARCH STANDARDS

4. The existing guidance frameworks for biorisk management at laboratories (including high-containment labs), such as the U.S. CDC's Biosafety in Microbiological and Biomedical Laboratories resource and WHO's Laboratory Biosafety Manual, do not include cyber risks. Biolabs and entities that oversee them must tighten cyber risk mitigation in coordination with biorisk management frameworks in order to minimize both the likelihood and impact of cyber attacks. For example, rapid incident response protocols and robust data backup can decrease the impact of an attack.[48] Additionally, private biolabs eschewing federal funding and select agents purchases do not fall under federal regulatory frameworks.[49]

5. Strengthening oversight of gain-of-function research can help mitigate severe cyber attack risks to biosecurity. The U.S. government should implement the National Science Advisory Board for Biosecurity (NSABB) report's dual-use research recommendations.[50] In particular, developing an integrated framework to identify concerning bioscience research would allow better assessment of cyber vulnerabilities. Also, clarifying policy

44 U.S. Cyberspace Solarium Commission. "Cyberspace Solarium Commission Report," March 2020.

45 Hay Newman, Lily. "The Hidden Race to Protect the US Bioeconomy From Hacker Threats." Wired, May 12, 2022.

46 Kouloufakos, Triantafyllos. "Digital Agriculture—A Gap in Critical Infrastructure Protection." Council on Foreign Relations, December 15, 2022.

47 Ibid.

48 Crawford, Elizabeth, Adam Bobrow, Landy Sun, Sridevi Joshi, Viji Vijayan, Stuart Blacksell, Gautham Venugopalan, and Nicole Tensmeyer. "Cyberbiosecurity in High-Containment Laboratories." Frontiers in Bioengineering and Biotechnology 11 (July 25, 2023).

49 Dan Greene , Jassi Pannu and Allison Berke. "The Danger of 'Invisible' Biolabs Across the U.S." Time, August 31, 2021.

50 National Science Advisory Board for Biosecurity. "Proposed Biosecurity Oversight Framework for the Future of Science," March 2023.

to mandate federal review of research that could enhance pathogen dangers through a cyber attack vector would close an oversight gap. The report also recommends strengthening international norms, which could make cyber threats in biological research a global priority.

SAFEGUARDING THE DIGITAL TO PHYSICAL FRONTIER

6. The Executive Branch's 2023 cybersecurity strategy calls for shifting liability onto software providers who fail to reasonably secure products, particularly for considering high-risk scenarios and preventing disclaimers of liability. As the Administration works with Congress and the private sector to draft this policy, biotech software and hardware should be explicitly included with stringent standards, with the aim of incentivizing the same security-by-design approach. Rapidly advancing biotech hardware, particularly those relating to the brain-computer interface for example, carry inherent vulnerabilities, as demonstrated in a 2013 experiment where a researcher remotely controlled another person's hand movements using a brain signal transmitted via the internet.[51]

7. Congress should direct HHS to evaluate regulations of gene synthesis products, and to require gene synthesis providers to enact screening protocols.[52] Congress should also consider requiring DNA synthesizers to implement stringent cybersecurity protections including intrusion detection systems, reduced screening windows to the minimum length required for DNA deobfuscation, rechecking fulfilled orders against new threat data, and increased data sharing to detect distributed malicious orders. Expanding voluntary initiatives like SecureDNA[53] along with instituting a trusted foundry model for genome sequencers, as proposed in the National Action Plan for U.S. Leadership in Biotechnology,[54] would establish end-to-end security standards ensuring genomic sciences remain resilient against potential threats throughout the supply chain.

BUILDING AWARENESS OF THREATS

8. Building public trust and countering disinformation through accurate information dissemination are vital components of an effective response to biological threats. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency should develop a coordinated communications campaign to improve public understanding and awareness of natural, deliberate, and accidental biological risks. It

51 The White House. "National Cybersecurity Strategy," March 2, 2023.

52 Congresswoman Anna Eshoo. "Rep. Eshoo, Sen. Markey Announce Health Security Agenda to Investigate Risks of Nuclear Weapons, Promote Safe Use of Gene Synthesis," July 18, 2023.

53 Rami Puzis, Dor Farbiash, Oleg Brodt, Yuval Elovici, and Dov Greenbaum. "Increased cyber-biosecurity for DNA synthesis." Nature Biotechnology, December 2020.

54 Special Competitive Studies Project. "National Action Plan for U.S. Leadership in Biotechnology," April 2023.

should work with behavioral scientists and communications experts, learning lessons from the COVID-19 pandemic to develop a coherent approach to increasing public awareness of risk.

CONCLUSION

The threats in the cyber-bio nexus demand immediate attention and robust policy responses. Legislative and regulatory efforts should focus on enhancing cybersecurity in critical sectors such as healthcare, biotech, and infrastructure. Additionally, stronger control and supervision of biosafety labs, increased information sharing, and effective governance of genomic data are essential. Balancing security measures with the need for innovation and responsible data sharing is crucial.

ABOUT THE AUTHOR

Abi Olvera is a Non-Resident Fellow with the Janne E. Nolan Center on Strategic Weapons at the Council on Strategic Risks.