INTERNATIONAL JOURNAL OF ADVANCED RESEARCH
ISSN: 3106-7980 : 3106-7972
Volume 3, Issue 4 [August, 2026]

CYBERBIOSECURITY: SECURING THE CONVERGENCE OF CYBER TECHNOLOGY AND BIOTECHNOLOGY

Dr. Sultan Salah-ud-Din[*1], Muhammad Aslam[2], Saqib Hussain[3]

[*1]*PhD in International Relations from the Department of Politics and International Relations, International Islamic University, Islamabad, Pakistan.*
[2]*PhD in International Relations and is a Visiting Research Scholar at the University of Massachusetts Amherst, USA.*
[3]*PhD in International Relations and is a Visiting Research Scholar at the University of Maryland, College Park, USA.*

[*1]sultansalahuddin01@gmail.com, [2]aslamkanwan5@gmail.com, [3]saqib.phdir62@iiu.edu.pk

DOI: https://doi.org/10.5281/zenodo.23154063

Keywords
Cyberbiosecurity, biosecurity, synthetic biology, DNA synthesis, bioeconomy, genomic data

Article History
Received: 16 May 2026
Accepted: 12 June 2026
Published: 15 August 2026

Copyright @Author
Corresponding Author: *
Dr. Sultan Salah-ud-Din

Abstract

Modern biology increasingly depends on digital technologies. Scientists design DNA using software, order biological materials through online platforms, conduct experiments with automated systems, and analyze results using networked computers. This connection between cyber technology and biotechnology creates benefits but also introduces new security risks. Cyberbiosecurity addresses these risks by protecting biological data, digital systems, laboratory equipment, and biotechnology processes from cyber threats and misuse. This paper examines cyberbiosecurity, identifies vulnerabilities across the biotechnology workflow, and reviews cyber threats documented in research. It also examines defenses at the technical, organizational, human, and policy levels. Using published studies and five figures, the paper shows how risks can move across stages of the biotechnology process. The study argues that cybersecurity should be integrated into biotechnology from the beginning rather than added after problems occur. Protection requires shared responsibility among laboratories, biotechnology companies, researchers, and governments. The paper concludes with priorities for strengthening cyberbiosecurity.

INTRODUCTION

Biotechnology is a rapidly growing part of the modern economy and supports medicines, vaccines, agriculture, clean fuels, and disease monitoring. Much of this work now depends on digital technologies. Scientists design DNA using software, order biological materials through online platforms, conduct experiments with automated equipment, and store results in large digital databases. As a result, modern biotechnology increasingly operates through connected digital systems. This creates important benefits but also new security risks. Cyber threats can affect biological research without direct physical access to a laboratory. For example, changes to digital files, false orders, or compromised software could disrupt research, expose sensitive information, or weaken safety controls. At the same time, the connection between biology and computing is becoming closer, as DNA can also be used to store digital information (Erlich & Zielinski, 2017).

Murch et al. (2018) introduced the term cyberbiosecurity to describe efforts to manage risks at the intersection of cybersecurity, cyber-physical security, and biosecurity. Peccoud et al. (2018) highlighted the importance of trust in the life sciences, where researchers depend on reliable suppliers, software, data, and professional networks. While this trust supports open and

efficient research, it can also create vulnerabilities when systems are misused or compromised. The issue is becoming more important as biotechnology expands and biological tools become more accessible. Carlson (2009) documented the declining cost of DNA synthesis, which has contributed to wider access to biotechnology. The COVID-19 pandemic also demonstrated the importance of secure health research, information, and digital systems (Mueller, 2021).

This paper has four main objectives. First, it defines cyberbiosecurity and explains its development. Second, it examines vulnerabilities across the biotechnology workflow. Third, it reviews major cyber threats identified or discussed in existing research. Finally, it examines available defenses and proposes practical measures for improving security. The paper uses published research and figures to explain how cyber risks can emerge and move across different stages of biotechnology. It avoids technical details that could facilitate harmful activities and instead focuses on understanding risks, strengthening protection, and promoting shared responsibility among researchers, laboratories, biotechnology companies, and policymakers.

What is Cyberbiosecurity?

Three Fields That Overlap

Cyberbiosecurity is easiest to understand as the overlap of three older ideas. The first is *cybersecurity*, which protects computers, networks, and data from theft, damage, or misuse. The second is *biosecurity*, which aims to prevent the harmful use or accidental release of dangerous biological agents and knowledge. The third is *cyber-physical security*, which protects machines that connect the digital world to the physical world, such as robots, pumps, sensors, and other laboratory equipment (Murch et al., 2018).

Each of these fields has its own experts, rules, and habits. Cybersecurity experts often know little about how a laboratory works. Biologists often know little about how attackers think. Biosecurity officials tend to focus on dangerous organisms and materials, not on software. Cyberbiosecurity tries to connect these groups so that no risk falls into the gaps between them. Figure 1 shows the overlap.

International Journal of Advanced Research

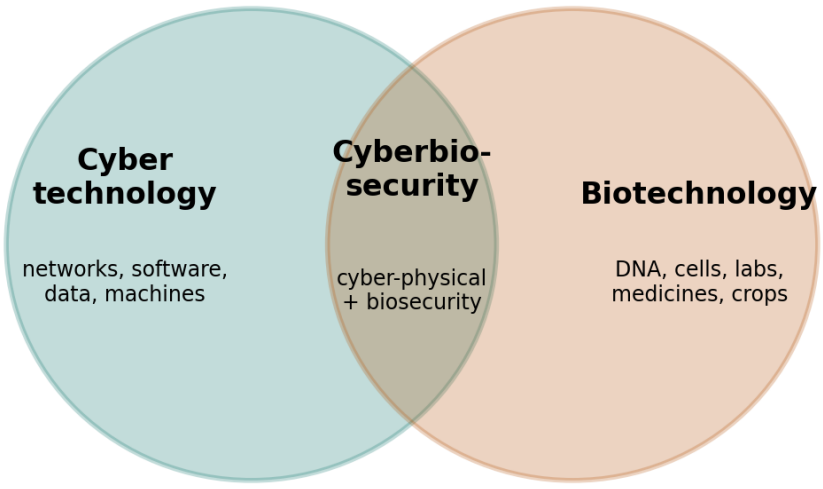


Figure 1 Cyberbiosecurity Sits Where Cyber Technology and Biotechnology Overlap

Note. The figure is a conceptual diagram based on the definition given by Murch et al. (2018).

How the Field Developed

Warnings about the mix of computers and biology started to appear in the middle of the 2010s, and the field took shape quickly after that. Figure 2 shows key steps in the studies discussed in this paper. In 2017, a research team showed that computer code could be hidden in synthetic DNA (Ney et al., 2017). In 2018, Murch et al. named and described the new field, Peccoud et al. explained the problem of naive trust, and the National Academies of Sciences, Engineering, and Medicine (NASEM, 2018) studied how progress in synthetic biology could change biological threats. In 2019, Vinatzer et al. looked at problems in pathogen genome databases. In 2020, Puzis et al. showed a weakness in DNA order screening. In 2021, Mueller discussed lessons from the pandemic. In 2023, the U.S. Department of Health and Human Services (HHS) released guidance for screening orders of synthetic nucleic acids.

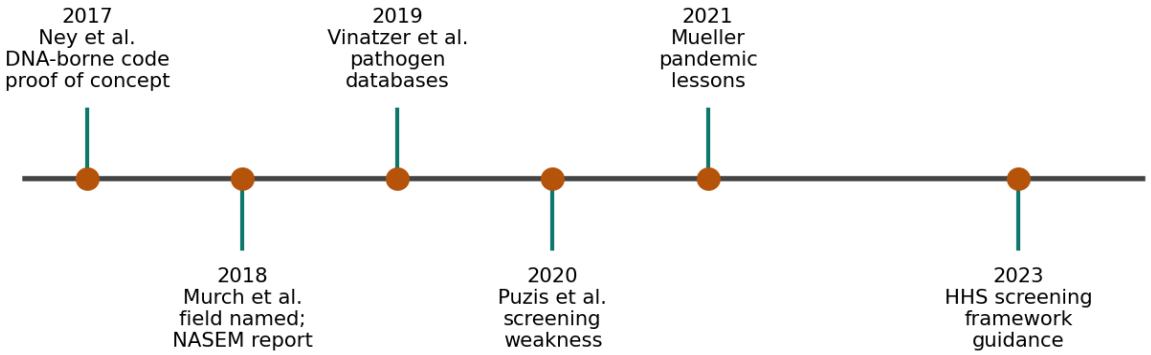


Figure 2 Selected Milestones in Cyberbiosecurity Research and Guidance

Note. The timeline shows only the works discussed in this paper. It is not a full history of the field.

The timeline shows a clear pattern. First, researchers showed that the risks were real. Next, they gave the field a name and a shared way of talking. Then they began to look at specific weak points, and later they moved toward guidance and rules. This is a common path for new areas of security, and it suggests that the field is still young and has much work ahead.

The Digital Life of Modern Biology

A Typical Workflow

To see where the risks are, it helps to follow a typical project from start to finish. Figure 3 shows the main steps. A project usually begins with a design. A scientist uses software to plan a DNA sequence, for example one that helps a microbe make a useful medicine. The next step is to get the DNA. Many laboratories place an online order with a company that makes DNA to order. The company usually checks the order to make sure it is safe before it builds the DNA.

Next comes building and testing. The DNA is put into cells, and the cells are grown and tested. Many laboratories use automated machines for this work, including liquid-handling robots and machines that control temperature and timing.

Some companies offer remote or "cloud" laboratories, where a customer sends instructions over the internet and machines carry them out. After testing, the scientist reads the DNA or other molecules with sequencing machines, which produce large data files. Finally, the results are stored, shared, and sometimes placed in public or private databases.

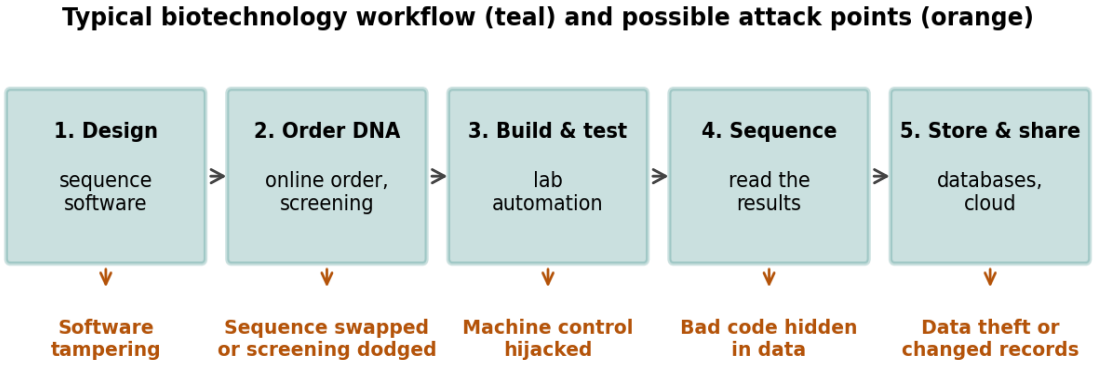


Figure 3 A Typical Biotechnology Workflow and Its Possible Attack Points

Note. The figure is a conceptual diagram by the author, based on ideas in Murch et al. (2018) and Peccoud et al. (2018).

Why This Creates Risk

Every step in the workflow uses digital tools, and every digital tool has flaws. Design software can be tampered with. Online ordering systems can be misused. Laboratory machines are often connected to networks so that they can be controlled from a distance, but many were built long before security was a concern. Sequencing machines produce data that must be processed by software. Databases hold valuable and sometimes private information. When these parts are joined into one chain, an attacker only has to find the weakest link.

There is a second reason for concern. In many industries, a security failure harms data or money. In biology, a failure can also harm living things. A hijacked machine could spoil a product, and a changed record could point scientists in the wrong direction. A dishonest actor could try to get a harmful biological material made by hiding the request. These outcomes are more serious than a stolen password, which is why biology needs its own security thinking and cannot simply copy the rules of other industries.

The bioeconomy also has a special feature: it is open and shared. Scientists often share data, methods, and materials freely because progress depends on it. That openness is a strength, but it makes strict control harder. The challenge for cyberbiosecurity is to add protection without shutting down the open exchange that makes science work.

Threats and Vulnerabilities

Researchers have described many kinds of risk. This section reviews the main ones, using published studies. It keeps the discussion at a general level and does not explain how to carry out an attack.

Attacks That Travel Through DNA Data

One of the best-known studies is the work of Ney et al. (2017). The team wanted to know whether the DNA itself could be used to attack a computer. They showed, in a controlled proof of concept, that computer code could be written into a piece of synthetic DNA. When a DNA sequencing program processed the data from that DNA, a flaw in the program let the hidden code take some control of the computer. The result was not an everyday threat. The conditions were carefully set up, and the authors said that real attacks would face many hurdles. Still, the study made an important point: data that comes from a biological sample should not be trusted blindly by software.

The same study looked at other problems, including privacy leaks from sequencing tools and the weak security of some bioinformatics software. Many scientific programs were written by researchers for their own use and were shared freely. They were never tested the way commercial security products are tested. This is a common and understandable gap, but it means that some widely used tools may have flaws that no one has looked for.

Getting Around DNA Screening

A second area of concern is the screening of DNA orders. Companies that make DNA usually compare each order against lists of dangerous sequences. Groups such as the International Gene Synthesis Consortium (IGSC, 2018) have set shared screening steps that member companies follow. The HHS (2023) guidance also encourages providers to screen both the sequences and the customers who ask for them.

Puzis et al. (2020) showed that these checks may have a blind spot. They described how malicious software on a customer's computer could change an order after the customer approved it. In their example, a harmless-looking request could be altered so that the company received something different. They also showed that certain screening methods could be fooled by small changes. The authors then proposed a stronger way to check orders. The lesson is that a security check is only useful if the data it checks is the true data, and that the whole chain from the customer's screen to the supplier's machine must be protected.

Data Theft and Privacy

Biological data is valuable. Drug designs, strain information, and research results can be worth a great deal to competitors or to foreign governments. Genetic data about people is also very personal. It can show family links and health risks, and it never changes. Gymrek et al. (2013) showed that a person's identity can sometimes be worked out from anonymous genetic data by combining it with public records. This means that removing a name from a data file does not always protect privacy.

Pathogen databases have their own problems. Vinatzer et al. (2019) explained that shared collections of pathogen genomes are very helpful for tracking disease outbreaks. But they raise questions about who may add data, who may see it, and how to tell whether a record has been changed. If the records in a public health database were altered, experts might draw wrong conclusions about where an outbreak began or how it was spreading. Keeping such data accurate and available is as important as keeping it private.

Attacks on Laboratory Machines and Production

Laboratory automation and manufacturing lines are the cyber-physical part of the problem. Murch et al. (2018) noted that machines in biotechnology are often linked to networks, and that they can run on old software that is hard to update. In drug making, timing and quality are critical, so a small change in machine settings could ruin a batch or hide a quality problem. Mueller (2021) also pointed out that health and research systems became more exposed during the pandemic, when many groups worked at high speed and with remote access.

Cloud laboratories raise a special question. When customers send instructions over the internet, the provider must make sure that each request is real, allowed, and safe. The provider must also protect the machines from being used in ways the owner did not intend. This is the same kind of trust problem seen in DNA ordering, only spread over a larger set of steps.

Insiders and Human Error

Not every problem comes from outside. Employees, students, and visitors often have access to valuable materials and systems. Most are honest, but a few might steal data or misuse equipment, and many more can make mistakes. Weak passwords, unpatched software, and unsafe use of personal devices are common in research settings. Peccoud et al. (2018) argued that a culture of trust makes it hard to ask colleagues to follow strict rules, and that this is one reason why human factors need attention.

Summary of Harms and Relative Risk

Table 1 groups the harms discussed above in simple terms. The groups are the author's own way of organizing the works cited and are not official categories.

Table 1 Main Types of Harm in Cyberbiosecurity

Type of harm	*Simple example*	*Source*
Code carried by data	Bad code hidden in DNA data attacks a sequencing program	Ney et al. (2017)
Screening bypass	An order is changed so a safety check is missed	Puzis et al. (2020)
Data theft and privacy loss	Identity worked out from "anonymous" genetic data	Gymrek et al. (2013)
Data tampering	Records in a pathogen database are altered	Vinatzer et al. (2019)
Process sabotage	A laboratory machine is hijacked and a batch is ruined	Murch et al. (2018)

Note. The grouping is the author's own way of organizing the sources listed.

Not every weak point is equally serious. Figure 4 gives a rough and illustrative ranking of the workflow steps by how likely a problem is and how large the effect could be. The scores are the author's judgment and were chosen only to show how a team might set priorities. They are not measured data. In this example, DNA ordering and databases score high because a failure could have wide effects and the systems are open to many users. A real organization should replace these scores with its own assessment.

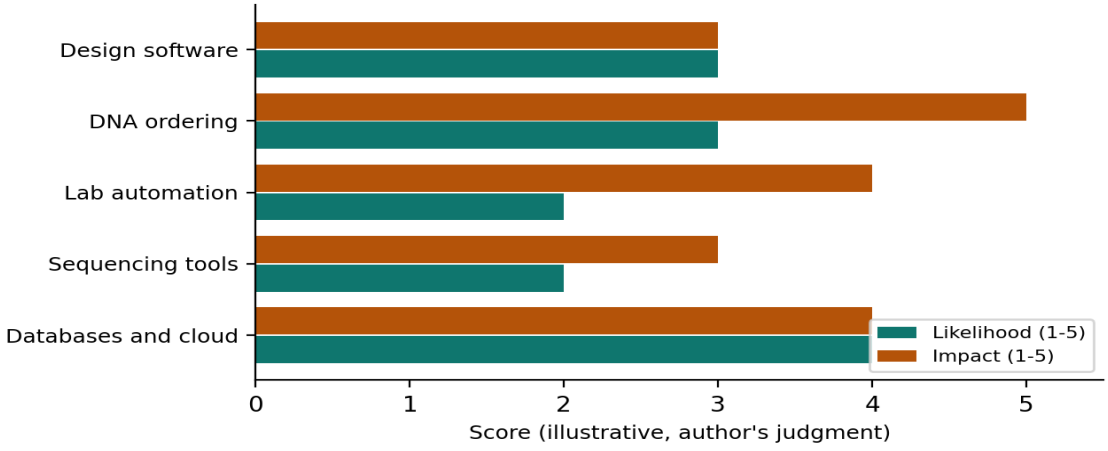


Figure 4 Illustrative Likelihood and Impact Scores for Workflow Steps

Who Might Attack, and Why

Different people have different reasons for attacking biological systems, and knowing them helps in planning a defense. Criminals may want money, for example by using ransomware to lock laboratory computers until a payment is made. Competitors or governments may want to steal designs and research results. Hackers may attack for fun or to show their skill. Insiders may be angry or may be paid to leak information. In a rarer and more serious case, a person or group might try to get a harmful biological material made by hiding the true purpose of an order.

Accidents matter as well. A mistake in a file, a software bug, or a poorly tested update can produce results that look just like an attack. For this reason, good security also helps with quality and safety, and the same controls often protect against both. A defender does not have to know who is behind a problem in order to prevent it.

The size of the threat is hard to judge. Public reports of attacks that affect biological materials are limited, and many organizations do not share incidents. The research described above mostly shows what is possible. It does not show how often attacks happen. This uncertainty is one reason why the field needs better reporting, and it is also a reason to be careful when making strong claims. A balanced view is that the risks are real and worth planning for, while the most extreme scenarios remain unlikely.

Defences

No single tool can secure the biotechnology workflow. Good defense uses several layers, so that if one layer fails, another still protects the system. This idea is often called defense in depth. Figure 5 shows the layers, with valuable assets in the center, technical controls around them, and people, rules, and sharing on the outside.



Figure 5 A Layered View of Cyberbiosecurity Defenses

Note. The figure is a concept map by the author.

Technical Controls

The first layer is basic cyber hygiene, and it is often the most useful. This means using strong and unique passwords, adding a second step to log-ins, keeping software up to date, and limiting who can reach which systems. Laboratory machines should

be placed on separate networks where possible, so that a problem in an office computer cannot spread to a robot. Sensitive data should be encrypted, and systems should keep logs so that strange activity can be seen later.

A helpful guide is the framework from the National Institute of Standards and Technology (NIST, 2018). It groups security work into five functions: identify what you have, protect it, detect problems, respond to them, and recover afterward. A laboratory can use this list as a checklist. It can begin by listing its machines, software, and data, which many groups find they have never done in full.

For DNA suppliers, the key control is careful screening. Following the ideas of the IGSC (2018) and the HHS (2023), providers can check both the order and the customer. The work of Puzis et al. (2020) adds a further step: providers should confirm that the final order matches what the customer approved, and customers should protect the computers used to place orders. For software that reads biological data, the lesson from Ney et al. (2017) is to treat the data as untrusted input. Developers can test programs for flaws and fix them before the programs are widely shared.

Detection and Response

Even strong defenses can fail, so laboratories also need to notice problems early and respond well. Simple steps help: watch logs for strange log-ins, check that machine settings have not changed, and compare important results against known good values. Each organization should also have a written plan that says who to call, which systems to isolate, and how to restore data from clean backups. Practicing the plan through short exercises shows weak spots before a real event. Recovery matters in biology because samples and cell lines can take months to replace. Backing up not only the data but also the records of how materials were made can save a great deal of time.

People and Culture

Technology alone is not enough. Scientists and technicians need short and practical training that explains the risks in their own language. They should know how to spot a suspicious message, how to report a problem, and why security rules exist. Peccoud et al. (2018) suggested that the shift from trust to awareness is mainly a matter of culture. Leaders can support this by making security part of normal lab work and by rewarding people who report problems instead of blaming them.

Education also matters over the long term. Universities can teach basic cybersecurity in biology programs and basic biology in computer science programs. Students who understand both areas will be the ones who build safer tools. Murch et al. (2018) listed education as one of the main needs of the new field.

Governance and Cooperation

The third layer includes laws, standards, and cooperation. NASEM (2018) argued that as synthetic biology grows, countries need better ways to judge new risks and to prepare for them. Clear standards help companies know what is expected. Shared guidance, such as the HHS (2023) framework, gives a starting point that many providers can follow. Because biology crosses borders, countries also need to work together, since an attacker can order from a supplier in one country while sitting in another.

Good governance also needs safe ways to share information. If a laboratory has an incident, others could learn from it, but many fear losing customers or reputation. Trusted reporting channels, with proper protection for those who report, could help the whole community learn faster. Table 2 summarizes the layers of defense and gives simple examples.

Table 2 Layers of Defense and Simple Examples

Layer	*Examples*	*Source*
Technical controls	Strong log-ins, software updates, separate lab networks, encryption, order matching	NIST (2018); Puzis et al. (2020)

Layer	*Examples*	*Source*
DNA screening	Checking sequences and customers before filling an order	IGSC (2018); HHS (2023)
People and culture	Short training, easy reporting, security as part of daily work	Peccoud et al. (2018)
Governance	Standards, shared guidance, international cooperation	NASEM (2018); HHS (2023)
Education	Security in biology courses and biology in security courses	Murch et al. (2018)

Note. The examples are summarized by the author from the works cited.

Challenges

Several problems make cyberbiosecurity hard. The first is a gap in skills. Few people have deep training in both biology and security, so the field lacks experts. The second is old equipment. Laboratory machines can cost a lot and last for many years, and their makers may not provide updates. A laboratory may be unable to fix a known flaw without replacing a machine.

The third problem is the balance between openness and control. Science moves faster when data and methods are shared. Strict rules can slow useful work, and they can push researchers to find ways around them. Good policy needs to protect against serious risks while leaving room for discovery. A related problem is that rules are not the same in every country, which allows an attacker to look for the easiest place to act.

The fourth problem is a lack of evidence. As noted above, there are few public data on incidents. Without data, it is difficult to know which defenses give the most benefit for their cost. Small laboratories and start-up companies face an extra difficulty because they have little money and few staff. They may see security as a distraction from their main mission. A useful answer is to provide free tools, templates, and training that fit small groups.

The fifth problem is that technology changes quickly. New methods for reading, writing, and editing DNA appear all the time, and new software tools follow. Defenses that work today may not work in a few years. Cyberbiosecurity therefore needs to be a habit of continued review and not a task that is finished once.

Recommendations and Future Directions

Based on the works reviewed here, several steps appear practical and useful. They are grouped by who can act.

Laboratories and companies should begin with a full list of their machines, software, and data, and should then apply basic cyber hygiene to each. They should place laboratory equipment on separate networks, keep software updated where they can, and control who has access. They should train all staff, including students and visitors, and give people an easy way to report problems. Companies that make DNA should keep screening both sequences and customers, and should check that orders are not changed before they arrive.

Software developers should treat all biological data as untrusted input. Tools should be tested for flaws and updated when problems are found. Funding agencies can help by paying for security review of widely used scientific programs, which are often built by small teams without a security budget.

Universities and schools should add short modules on security to biology courses, and basic biology to security courses. Joint projects and exercises, in which biologists and security experts work together, are a good way to build shared understanding.

Governments and international bodies should support clear standards, share guidance, and create safe reporting channels. They should also fund

research that measures the real size of the risks, so that limited money can be spent where it does the most good. Cooperation across borders should be a priority, because the supply chains of biotechnology are global.

Researchers should continue to study the weak points in the workflow, and should share their findings responsibly. This means telling the makers of a tool about a flaw before publishing details, and describing risks in a way that helps defenders more than attackers. Future work could also test defenses in real laboratories, compare the cost and benefit of different controls, and study how well training changes behavior.

Conclusion

Biotechnology and cyber technology are now closely connected. This connection makes scientific work faster, easier, and cheaper, but it also creates new risks. Biological data, computer systems, and laboratory machines can be misused or attacked if they are not properly protected. Cyberbiosecurity helps us understand and manage these risks together. The best way to stay safe is to use several layers of protection, including secure computer systems, trained staff, careful handling of data, clear rules, and quick reporting of problems. These security measures do not have to stop scientific progress. Instead, they can build trust and help science and the biotechnology industry grow safely. If laboratories, companies, and governments work together and include security from the beginning, the bioeconomy can develop in a way that is useful, innovative, and safe.

REFERENCES

Carlson, R. (2009). The changing economics of DNA synthesis. *Nature Biotechnology, 27*(12), 1091–1094. https://doi.org/10.1038/nbt1209-1091

Erlich, Y., & Zielinski, D. (2017). DNA Fountain enables a robust and efficient storage architecture. *Science, 355*(6328), 950–954. https://doi.org/10.1126/science.aaj2038

Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying personal genomes by surname inference. *Science, 339*(6117), 321–324. https://doi.org/10.1126/science.1229566

International Gene Synthesis Consortium. (2018). *Harmonized screening protocol v2.0: Gene synthesis consortium*.

Mueller, S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? *Biosafety and Health, 3*(1), 11–21.

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology, 6*, Article 39. https://doi.org/10.3389/fbioe.2018.00039

National Academies of Sciences, Engineering, and Medicine. (2018). *Biodefense in the age of synthetic biology*. The National Academies Press. https://doi.org/10.17226/24890

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://doi.org/10.6028/NIST.CSWP.04162018

Ney, P., Koscher, K., Organick, L., Ceze, L., & Kohno, T. (2017). Computer security, privacy, and DNA sequencing: Compromising computers with synthesized DNA, privacy leaks, and more. In *Proceedings of the 26th USENIX Security Symposium* (pp. 765–779). USENIX Association.

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: From naive trust to risk awareness. *Trends in Biotechnology, 36*(1), 4–7. https://doi.org/10.1016/j.tibtech.2017.10.012

Puzis, R., Farbiash, D., Brodt, O., Elovici, Y., & Greenbaum, D. (2020). Increased cyber-biosecurity for DNA synthesis. *Nature Biotechnology, 38*(12), 1379–1381. https://doi.org/10.1038/s41587-020-00761-y

International Journal of Advanced Research

U.S. Department of Health and Human Services. (2023). *Screening framework guidance for providers and users of synthetic nucleic acids*.

Vinatzer, B. A., Heath, L. S., Almohri, H. M. J., Stulberg, M. J., Lowe, C., & Li, S. (2019). Cyberbiosecurity challenges of pathogen genome databases. *Frontiers in Bioengineering and Biotechnology*, 7, Article 106. https://doi.org/10.3389/fbioe.2019.00106

International Journal of Advanced Research