Biosecurity Risks Associated with Emerging Laboratory Technologies

Shaukat Khan[1,*], Murad Khan [1], Palwasha Khan[1], Asghar Ali[1] and Hizqeel Ahmed Muzaffar[2]

[1]Association for Biorisk Management-Pakistan
[2]KBCMA College of Veterinary and Animal Sciences, Narwal (Sub-campus) UVAS, Lahore
*Corresponding author: Shaukat.khan@hsp-pakistan.org

Abstract

As the world advances towards emerging laboratory techniques and technological advancement, the risks associated with biosecurity are also arising. Although there is implementation of biosecurity protocols within laboratory settings, technological advancement is continuously imposing risks associated with biosecurity. Biosecurity breaches such as bioterrorism and biowarfare are common forms of biosecurity risks. Bioterrorism agents can now be developed in a laboratory setting because of emerging laboratory technologies. Poor biosecurity within a laboratory setting leads to the release of harmful agents in the external environment. As the world is becoming connected through the internet, cyber-attacks are great threats to laboratory data. Cyber penetration into the laboratory's data can lead to harmful consequences such as data theft and data leaks. There is also potential harmful use of proteomics, genomics, and bioinformatics data through cyber-attacks. Emerging laboratory technologies such as CRISPR, synthetic biology, and genetic engineering can lead to the development of harmful infectious agents such as polio virus and horsepox virus. There is a need for strict policies to regulate the biosecurity risks regarding emerging laboratory technologies.

Keywords: Laboratory, Biosecurity, Risks, Emerging, Cyber, Bioterrorism

Cite this Article as: Khan S, Khan M, Khan P, Ali A and Muzaffar HA, 2025. Biosecurity risks associated with emerging laboratory technologies. In: Farooqi SH, Kholik K and Zaman MA (eds), One Health Horizons: Integrating Biodiversity, Biosecurity, and Sustainable Practices. Unique Scientific Publishers, Faisalabad, Pakistan, pp: 170-175. https://doi.org/10.47278/book.HH/2025.122

A Publication of Unique Scientific Publishers

Chapter No: 25-023

Received: 25-Jan-2025
Revised: 15-Apr-2025
Accepted: 29-May-2025

Introduction

Since the global outbreak of COVID-19, worldwide concerns regarding biosecurity have increased (Huang et al., 2021; Ding et al., 2022). Patient care usually requires laboratory testing. However, clinical professionals don't know about the presence of infectious agents in the samples, as a result, biosecurity has to be ensured by the professionals performing laboratory tests (Cornish et al., 2021). Within any laboratory testing, infectious agents, standard operating procedures, reagents, and instrumentation are evaluated to determine any potential hazards. Biosecurity considerations are always in mind to reduce the potential risks (Aspland et al., 2021). Biosecurity is associated with a set of precautionary measures to handle pathogenic microbial strains safely within a laboratory (Peng et al., 2018). Pathogenic infectious agents have remained a major source of infection and mortality among laboratory workers despite greater awareness. The harms associated with these pathogenic agents can be minimized by strictly following the biosecurity protocols (Artika & Ma'roef, 2017). As laboratory capacity is increasing worldwide, global health is now associated with biosecurity (Bakanidze et al., 2010). Biosecurity is related to the protection, accountability, and control measures adapted for the prevention of theft, loss, misuse, or intentional release of pathogens (Dickmann et al., 2015). Laboratory biosecurity is essential to ensure a researcher's safety from laboratory-acquired infections and the protection of the general public from intentional or unintentional exposure to infectious agents (Gaudioso & Zemlo, 2007). The status of biosecurity within a laboratory setting can be evaluated by ensuring the general knowledge of laboratory biosecurity, proper use of personal protection equipment, management knowledge of biological safety, adherence to standard laboratory protocols, and awareness level among the persons working in the laboratory (Odetokun et al., 2017). Personnel, physical, material, and information controls are the four basic controls of biosecurity (Muneer et al., 2021).

Biosecurity protocols are not always based on clear evidence. Unnecessary procedures may be adapted because of the gaps in nonevidence and evidence-based approaches. This can increase costs and create challenges within laboratories (Blacksell et al., 2023). Because of the increase in biosecurity issues within laboratories in recent years, the culture of responsibility among the workers has been promoted (Perkins et al., 2019). As the research on pathogenic agents such as parasites, fungi, bacteria, and viruses is increasing there is a global risk of emerging biological risks not only related to people but also to the environment (Coelho & García Díez, 2015). Emerging infectious diseases pose significant threats to human beings and their surroundings. In addition, biological warfare, bioterrorism, biological accidents, and harmful consequences arising from dual-use biotechnology also pose a challenge to biosecurity. Improving the early surveillance capabilities is necessary for building a common biosecurity shield for the worldwide community of health (Hao et al., 2022). In order to improve biosecurity in a laboratory, it is essential to address the developing challenges, ultimately finding a solution to reduce the biosecurity risks (Meulenbelt et al., 2019). This chapter discusses the biosecurity risks that are associated with emerging laboratory technologies so that their solutions can be planned.

1. Biosecurity Risks Associated with Emerging Laboratory Technologies

1.1. Laboratory Biosecurity Breaches

The successful implementation of biosecurity depends upon the commitment of a community towards following the biosecurity principles and a proper understanding and knowledge regarding the biosecurity. With the development of biosecurity checklist, necessary steps have to be taken in order to implement them. This can be achieved by evaluating the current biosecurity levels. It is very important to avoid biosecurity breaches, bioterrorism, and biological warfare (Brizee et al., 2019). Facilities for bioscience are essential for the fight against bioterrorism and infectious diseases that arise unexpectedly. However, how bioscience organizations handle the safety and security hazards of organisms that cause infectious diseases is being questioned by the public and policymakers. As a result, the way bioscience operates is being directly impacted by new national rules in many countries as well as international initiatives from the World Health Organization, the United Nations, and others. For bioscience facilities, which have a responsibility to guarantee the safe and secure operation of their facilities, laboratory biosecurity is a relatively new and developing concept (Gaudioso et al., 2009). Bioterrorism agents such as *Bacillus anthracis*, *Yersinia pestis*, *Brucella*, *Burkholderia mallei*, and *Burkholderia pseudomallei* are greater threats to the community as these can be easily grown now in the laboratories (Wagar, 2016). As the handling of microbial agents within a laboratory setting may be dangerous, some of the biohazards may be laboratory-acquired (Ishaque et al., 2021; Laith & Alnemri, 2022).

Furthermore, chemical hazards may be associated with the corrosive, mutagenic, and toxic substances used as reagents in the laboratories (Nieuwenweg et al., 2021). There is a lack of development of laboratories equipped with biosafety level 4 which is essential to response to future threats (Michalski et al., 2022). Because of concerns about bioterrorism and emerging infectious diseases, the world is now focusing on ensuring biosecurity within a laboratory (Gao et al., 2024). Rapidly expanding technological skills and the more rapid evolution of molecular biological disciplines and biotechnology sometimes lead to the development of bioterrorism threats. Another significant element that contributes to the complexity of the situation is the quick growth of transnational terrorist groups and their access to resources, tools, and knowledge necessary to create biological weapons. Therefore, to minimize negative health impacts and prevent fatalities, a bioterrorism danger needs to be recognized and addressed (Krishan et al., 2017; Wani et al., 2022). A bioweapon production facility is essentially a regular microbiological lab on a smaller scale. With the use of genetic engineering techniques, research on microbes in pathology and epidemiology that leads to the creation of a vaccine to stop and manage the disease outbreak could be purposefully used to create vaccine-resistant strains for use in terrorism or conflict (Aduojo et al., 2022). Poor biosecurity within a laboratory causes the release of harmful agents (Barras & Greub, 2014; Reardon, 2014; Rathjen & Shahbodaghi, 2021). People can be protected by following specified guidelines while applying biosecurity laboratory measures. Through data collection, analysis, and distribution, medical intelligence plays a critical role in tracking and evaluating the threat of bioterrorism. By comprehending and putting into practice strict biosecurity procedures in labs, the medical intelligence community may contribute to preventing bioterrorism and preserving public safety. Medical intelligence must prepare for bioterrorism attacks, which can happen at any time, by researching and evaluating bioterrorism threats, analyzing data so that the government can implement the necessary policies to promptly detect and track the spread of infectious diseases, and creating disease prevention plans (Subariyah et al., 2023).

1.2. Cybersecurity Risks

As organizations are becoming dependent upon networks, clinical laboratories, and healthcare organizations are now becoming vulnerable to cyber-attacks (Patel et al., 2023). Cyber penetration of lab equipment provides access to the laboratory's sensitive scientific data. Access to laboratory equipment such as incubators, refrigerators, and freezers can lead to the destruction of valuable reagents and microorganisms. Furthermore, protein and genomic sequences present in electronic devices may be altered, misused, destroyed, or theft (Reed & Dunaway, 2019). In the era of rapidly advancing laboratories, biotechnology, and medical research, the use of interconnected technologies for patient care and health is causing these laboratories to become vulnerable to cyber-attacks (Huff et al., 2023). Internet-connected instruments and applications of software in the medical field are causing their increased vulnerability to cyber-attacks (Bhatia, 2024). Healthcare systems are at greater risk of cyber-attacks due to the sensitivity of the information present in the healthcare systems. As the laboratories are now using information technology, digitization, and computerization, they are highly vulnerable to cyber-attacks (Lippi et al., 2025). High-containment laboratories carry out critical research on infectious diseases, produce vaccines, and provide diagnostic services for high pathogenic agents. The modernization of these laboratories has made their infrastructure depend upon cyber-connected networks (Crawford et al., 2023). As these laboratories create critical data, they become vulnerable to cybersecurity concerns (Bhushan, 2023). Cyber-attacks can adversely affect the genomics data (Sheldon et al., 2024). Medical devices are now connected with communication and information technology. However, this advancement in technology is causing internal and external security threats (Kim et al., 2020). Devices that communicate with the internet for operation can be attacked by cyber-attacks. Such a cyber-attack can lead to harmful consequences such as data theft and patient harm (Badrouchi et al., 2020).

Biological laboratories, facilities, storage systems, data transfer systems, software for data analysis programs, integration systems for biological research, systems for improving healthcare, and pathogen surveillance systems are at risk of cyber-attacks (Berger, 2020). Biotechnology has become more accessible and novel treatments have been developed more quickly. Thanks to the convergence of biotechnology advancements with laboratory automation, data access, and computational biology. Yet, the digital age's expanded availability of biotechnology has also raised new security issues, leading to the development of the field of cyberbiosecurity, which combines biosecurity, cyber-physical security, and cybersecurity. With the rise of this new field, a rational, repeatable, and collaborative method for assessing system and facility vulnerabilities to cyberbiosecurity threats is required (Schabacker et al., 2019). Healthcare point-of-care systems, which have been extensively utilized in hospitals to offer medical experts cutting-edge solutions, are one important factor to take into account when it comes to cybersecurity and privacy issues. Point-of-care systems give clinicians a comprehensive picture of patients' status, facilitating prompt responses and avoiding emergency circumstances. Point-of-care systems are platforms that use gadgets and software to gather, process, and display data. It becomes clear that numerous threats could result in data leaks or breach incidents when massive volumes of data, including private health

information and sensitive medical data are shared across different systems (Jofre et al., 2021). With the proliferation of proactive mobile healthcare, the market for wireless biomedical devices such as wearables, implantables, ingestibles, and different injectables is growing quickly. Although the expansion of wireless biomedical devices expands the range of medical services available, the use of these technologies puts users' privacy and security at risk (Vakhter et al., 2022). As the threats of cyber-attacks on laboratories are increasing day by day, rapid actions have to be taken (Ayala, 2016).

1.3. Genetic Engineering

In addition to the advancements in science and technology in laboratories, the production of new microorganisms is now possible which is a great threat to humanity (Trump et al., 2020a). The advancements in genomics, proteomics, and bioinformatics now have abused use (Fatollahi Arani & Zeinoddini, 2023). Synthetic biology provides support for the development of dangerous infectious agents. It has now become possible to obtain the whole genome sequence of lethal pathogenic agents. Furthermore, the methods of increasing the pathogenicity of infectious agents are now described. Barriers to the development of infectious agents now have been removed (Wang & Zhang, 2019; Wang et al., 2021). It was reported that the abusers were able to synthesize horsepox virus through the DNA fragments ordered online (Medaglia et al., 2015). CRISPR technology has also undefined health consequences (Yin et al., 2018; Zhang et al., 2018). It is currently hard to measure the degree of exposure to synthetic biology hazards. We are unable to predict with certainty which platform could be utilized to create a biological weapon or danger. We also have no way of knowing who a biological strike will target. Third, we don't know how the weapon will be used against the target, therefore it's difficult to forecast the effects of release. The use of aerosolized spray containing the disease at the center of mass transit or transferring a computer virus encoded in genetic material to a specialized laboratory for computer hacking upon sequencing are some possible strategies (Trump et al., 2020b). After being released from the laboratory, genetically engineered microorganisms have indirect or direct effects on the external environment (Zhou et al., 2019). Any virus can now be developed in the laboratory with the help of genetic engineering (Gómez-Tatay & Hernández-Andreu, 2019).

Table 1: Biosecurity risks associated with emerging laboratory technologies

Biosecurity risks	Reference
Biosecurity breaches, bioterrorism, and biowarfare	Brizee et al., 2019
Bioterrorism	Gaudioso et al., 2009; Subariyah et al., 2023; Gao et al., 2024
Bioterrorism agents such as *Bacillus anthracis*, *Yersinia pestis*, *Brucella*, *Burkholderia mallei*, and *Burkholderia pseudomallei*	Wagar, 2016
Biohazards	Ishaque et al., 2021; Laith & Alnemri, 2022; Laith & ALnemri, 2022
Chemical hazards	Nieuwenweg et al., 2021
Bioterrorism, biological weapons	Krishan et al., 2017; Wani et al., 2022
Biological weapon	Aduojo et al., 2022
Release of harmful agents	Barras & Greub, 2014; Reardon, 2014; Rathjen & Shahbodaghi, 2021
Cyber attacks	Ayala, 2016; Berger, 2020; Patel et al., 2023; Huff et al., 2023; Bhatia, 2024; Lippi et al., 2025
Access to the laboratory's sensitive scientific data	Reed & Dunaway, 2019
Cybersecurity concerns	Schabacker et al., 2019; Bhushan, 2023
Threats to the genomics data	Sheldon et al., 2024
Internal and external security threats	Kim et al., 2020
Data theft	Badrouchi et al., 2020
Data leaks	Jofre et al., 2021
Privacy concerns	Vakhter et al., 2022
Production of new microorganisms	Trump et al., 2020a
Abused use of proteomics, genomics, and bioinformatics	Fatollahi Arani & Zeinoddini, 2023
Development of dangerous infectious agents	Wang & Zhang, 2019; Wang et al., 2021
Development of horsepox virus	Medaglia et al., 2015
Undefined health consequences	Yin et al., 2018; Zhang et al., 2018
Hazards of synthetic biology	Trump et al., 2020b
Genetically engineered microorganisms	Zhou et al., 2019
Development of viruses	Gómez-Tatay & Hernández-Andreu, 2019
Development of superbugs	Van Puyvelde et al., 2018
Development of polio virus	Jameel, 2011; Sun et al., 2022
Hazards of CRISPR technology	West & Gronvall, 2020
Development of synthetic viruses	Maclntyre, 2015

Genetically engineered microorganisms can lead to the development of superbugs if they are released in the external environment (Van Puyvelde et al., 2018). Polio vrius has now been developed through synthetic biology (Jameel, 2011; Sun et al., 2022). The biological sciences and medical research are being transformed by the potent gene-editing technology known as CRISPR. Additionally, the technology has been made more accessible. The cost of using CRISPR is inexpensive and steadily declining, kits are readily available to make the process simple, and the body of scientific literature on CRISPR techniques and innovative applications is expanding quickly. But like other significant developments

in the life sciences, CRISPR presents biosecurity issues because it might be abused and because it reduces the technical obstacles to the production of biological weapons, highlighting the hazards to biosecurity (West & Gronvall, 2020). Our biosecurity is at risk due to the fact that our systems, thinking, education, legislation, and policies are falling far behind significant scientific advancements. The threat to global biosecurity is being addressed by the need for new systems, legislation, productive operational models, and ways of thinking. Synthetic viruses and genetic engineering of pathogens are real, and dual-use science is rapidly accelerating. The public availability of dual-use genetic engineering methods, along with the insider threat, presents an unprecedented risk to biosecurity (MacIntyre, 2015). Raising awareness of the biological risks connected to laboratory activity or the improper use of biotechnology is a first and crucial step in achieving biosafety and biosecurity sustainability. In any nation that uses biotechnology, increasing awareness can help implement biosafety and biosecurity concepts by expanding the capacity to recognize and address potential biohazards that are not yet known (Laith & ALnemri, 2022). Biosecurity risks associated with emerging laboratory technologies have been summarized below in Table 1.

Conclusion

As there has been a great advancement in the field of research and laboratory techniques within the past few years, there are also limitations associated with this advancement. Biosecurity risks are one of them. Although the worldwide focus is on the maintenance of biosecurity protocols within a laboratory, there is still a need for the development of protocols in order to prevent biosecurity breaches such as bioterrorism, biowarfare, data leak and data theft as these breaches can lead to harmful consequences. As the world becomes interconnected through internet networks, they become vulnerable to cyber-attacks. Furthermore, synthetic biology such as genetic engineering can lead to the development of harmful infectious agents which is a great threat to humanity.

References

Aduojo, E. E., Amina, S. B., Kemi, O., & Jabir, A. (2022). Bioterrorism and biodefence: Biotechnology and security implications for Nigeria. *Am. Journal Bioterror Biosecur Biodefens*, *5*, 1-5. https://www.researchgate.net/profile/Amina-Bature/publication/360121455

Artika, I. M., & Ma'roef, C. N. (2017). Laboratory biosafety for handling emerging viruses. *Asian Pacific Journal of Tropical Biomedicine*, *7*(5), 483-491. https://doi.org/10.1016/j.apjtb.2017.01.020

Aspland, A. M., Douagi, I., Filby, A., Jellison, E. R., Martinez, L., Shinko, D., & Thornton, S. (2021). Biosafety during a pandemic: shared resource laboratories rise to the challenge. *Cytometry Part A*, *99*(1), 68-80. https://doi.org/10.1002/cyto.a.24280

Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities. *Berkeley, CA*. ISBN : 978-1-4842-2154-9. https://doi.org/10.1007/978-1-4842-2155-6

Badrouchi, F., Aymond, A., Haerinia, M., Badrouchi, S., Selvaraj, D. F., Tavakolian, K., & Eswaran, S. (2020). Cybersecurity vulnerabilities in biomedical devices: A hierarchical layered framework. *Internet of Things use Cases for the Healthcare Industry*, 157-184. https://doi.org/10.1007/978-3-030-37526-3_7

Bakanidze, L., Imnadze, P., & Perkins, D. (2010). Biosafety and biosecurity as essential pillars of international health security and cross-cutting elements of biological nonproliferation. *BMC Public Health*, *10*, 1-8. https://doi.org/10.1186/1471-2458-10-S1-S12

Barras, V., & Greub, G. (2014). History of biological warfare and bioterrorism. *Clinical Microbiology and Infection*, *20*(6), 497-502. https://doi.org/10.1111/1469-0691.12706

Berger, K. M. (2020). Addressing cyber threats in biology. *IEEE Security & Privacy*, *18*(3), 58-61. https://doi.org/10.1109/MSEC.2020.2966110

Bhatia, S. (2024). Cybersecurity Threats in Medical Laboratories: Time to Take Precautions. *Medical Science and Discovery*, *11*(6), 177-179. http://dx.doi.org/10.36472/msd.v11i6.1166

Bhushan, M. (2023). Cyber-biosecurity. *J. Defense Stud*, *17*(2), 93-119. https://idsa.demosl-03.rvsolutions.in/system/files/jds/jds-17-2_Mrinmayee-Bhushan.pdf

Blacksell, S. D., Dhawan, S., Kusumoto, M., Le, K. K., Summermatter, K., O'Keefe, J., & Hamilton, K. (2023). The Biosafety Research Road Map: The search for evidence to support practices in human and veterinary laboratories. *Applied Biosafety*, *28*(2), 64-71. https://doi.org/10.1089/apb.2022.0040

Brizee, S., Passel, M. W. V., Berg, L. M. V. D., Feakes, D., Izar, A., Lin, K. T. B., & Bleijs, D. A. (2019). Development of a biosecurity checklist for laboratory assessment and monitoring. *Applied Biosafety*, *24*(2), 83-89. https://www.liebertpub.com/doi/epub/10.1177/1535676019838077

Coelho, A. C., & García Díez, J. (2015). Biological risks and laboratory-acquired infections: a reality that cannot be ignored in health biotechnology. *Frontiers in Bioengineering and Biotechnology*, *3*, 56. https://doi.org/10.3389/fbioe.2015.00056

Cornish, N. E., Anderson, N. L., Arambula, D. G., Arduino, M. J., Bryan, A., Burton, N. C., & Campbell, S. (2021). Clinical laboratory biosafety gaps: lessons learned from past outbreaks reveal a path to a safer future. *Clinical microbiology reviews*, *34*(3), 10-1128. https://doi.org/10.1128/cmr.00126-18

Crawford, E., Bobrow, A., Sun, L., Joshi, S., Vijayan, V., Blacksell, S., & Tensmeyer, N. (2023). Cyberbiosecurity in high-containment laboratories. *Frontiers in Bioengineering and Biotechnology*, *11*. https://doi.org/10.3389/fbioe.2023.1240281

Dickmann, P., Sheeley, H., & Lightfoot, N. (2015). Biosafety and biosecurity: a relative risk-based framework for safer, more secure, and sustainable laboratory capacity building. *Frontiers in Public Health*, *3*, 241. https://doi.org/10.3389/fpubh.2015.00241

Ding, J., Xiao, H., & Chen, X. (2022). Advanced biosafety materials for prevention and theranostics of biosafety issues. *Biosafety and Health*, *4*(02), 59-60. https://doi.org/10.1016/j.bsheal.2022.03.011

Fatollahi Arani, S., & Zeinoddini, M. (2023). Gene editing: biosecurity challenges and risks. *Journal of Police Medicine*, *12*(1), 1-19. https://jpmed.ir/article-1-1171-en.html

Gao, W., Wu, Z., Zuo, K., Xiang, Q., Zhang, L., Chen, X., & Liu, H. (2024). From biosafety to national security: The evolution and challenges of

biosafety laboratories. *Laboratories*, *1*(3), 158-173. https://doi.org/10.3390/laboratories1030013

Gaudioso, J., & Zemlo, T. (2007). Survey of bioscience research practices in Asia: implications for biosafety and biosecurity. *Applied Biosafety*, *12*(4), 260-267. https://www.liebertpub.com/doi/abs/10.1177/153567600701200408

Gaudioso, J., Gribble, L. A., & Salerno, R. M. (2009). Biosecurity: Progress and challenges. *JALA: Journal of the Association for Laboratory Automation*, *14*(3), 141-147. https://doi.org/10.1016/j.jala.2009.01.001

Gómez-Tatay, L., & Hernández-Andreu, J. M. (2019). Biosafety and biosecurity in synthetic biology: a review. *Critical reviews in environmental science and technology*, *49*(17), 1587-1621. https://doi.org/10.1080/10643389.2019.1579628

Hao, R., Liu, Y., Shen, W., Zhao, R., Jiang, B., Song, H., & Ma, H. (2022). Surveillance of emerging infectious diseases for biosecurity. *Science China Life Sciences*, *65*(8), 1504-1516. https://doi.org/10.1007/s11427-021-2071-x

Huang, X., Xu, W., Li, M., Zhang, P., Zhang, Y. S., Ding, J., & Chen, X. (2021). Antiviral biomaterials. *Matter*, *4*(6), 1892-1918. https://doi.org/10.1016/j.matt.2021.03.016

Huff, A. J., Burrell, D. N., Nobles, C., Richardson, K., Wright, J. B., Burton, S. L., & Brown-Jackson, K. L. (2023). Management Practices for Mitigating Cybersecurity Threats to Biotechnology Companies, Laboratories, and Healthcare Research Organizations. In *Applied Research Approaches to Technology, Healthcare, and Business,* 1-12. 10.4018/979-8-3693-1630-6.ch001

Ishaque, S., Asrhad, A., Haider, M. A., & Fatima, F. (2021). Biosafety and biosecurity of lab and hospital acquired infections. *Biological and Clinical Sciences Research Journal*, *2021*(1). e008. https://doi.org/10.54112/bcsrj.v2021i1.55

Jameel, S. (2011). Ethics in biotechnology and biosecurity. *Indian Journal of Medical Microbiology*, *29*(4), 331-335. https://doi.org/10.4103/0255-0857.90155

Jofre, M., Navarro-Llobet, D., Agulló, R., Puig, J., Gonzalez-Granadillo, G., Mora Zamorano, J., & Romeu, R. (2021). Cybersecurity and privacy risk assessment of point-of-care systems in healthcare—a use case approach. *Applied Sciences*, *11*(15), 6699. https://doi.org/10.3390/app11156699

Kim, D. W., Choi, J. Y., & Han, K. H. (2020). Medical device safety management using cybersecurity risk analysis. *IEEE Access*, *8*, 115370-115382. https://doi.org/10.1109/ACCESS.2020.3003032

Krishan, K., Kaur, B., & Sharma, A. (2017). India's preparedness against bioterrorism: biodefence strategies and policy measures. *Current Science*, 1675-1682. https://www.jstor.org/stable/26493307

Laith, A. E., & Alnemri, M. (2022). Biosafety and biosecurity in the era of biotechnology: The Middle East region. *Journal of Biosafety and Biosecurity*, *4*(2), 130-145. https://doi.org/10.1016/j.jobb.2022.11.002

Lippi, G., Akhvlediani, S., Cadamuro, J., Danese, E., de Guadiana Romualdo, L. G., Delacour, H., & Plebani, M. (2025). EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) recommendations for reinforcing cyber-security and managing cyber-attacks in medical laboratories. *Clinical Chemistry and Laboratory Medicine (CCLM)*, *63*(1), 27-34. https://doi.org/10.1515/cclm-2024-0803

MacIntyre, C. R. (2015). Biopreparedness in the age of genetically engineered pathogens and open access science: an urgent need for a paradigm shift. *Military Medicine*, *180*(9), 943-949. https://academic.oup.com/milmed/article/180/9/943/4160600

Medaglia, M. L. G., Moussatché, N., Nitsche, A., Dabrowski, P. W., Li, Y., Damon, I. K., & Damaso, C. R. (2015). Genomic analysis, phenotype, and virulence of the historical Brazilian smallpox vaccine strain IOC: implications for the origins and evolutionary relationships of vaccinia virus. *Journal of Virology*, *89*(23), 11909-11925. https://doi.org/10.1128/jvi.01833-15

Meulenbelt, S. E., Van Passel, M. W., De Bruin, A., Van den Berg, L. M., Schaap, M. M., Rutjes, S. A., & Bleijs, D. A. (2019). The Vulnerability Scan, a web tool to increase institutional biosecurity resilience. *Frontiers in Public Health*, *7*, 47. https://doi.org/10.3389/fpubh.2019.00047

Michalski, A., Knap, J., Bielawska-Drózd, A., & Bartoszcze, M. (2022). Lessons learned from 2001-2021-from the bioterrorism to the pandemic era. *Annals of Agricultural and Environmental Medicine*, *29*(1). 1-11. http://dx.doi.org/10.26444/aaem/146604

Muneer, S., Kayani, H. A., Ali, K., Asif, E., Zohra, R. R., & Kabir, F. (2021). Laboratory biosafety and biosecurity related education in Pakistan: Engaging students through the Socratic method of learning. *Journal of Biosafety and Biosecurity*, *3*(1), 22-27. https://doi.org/10.1016/j.jobb.2021.03.003

Nieuwenweg, A. C., Trump, B. D., Klasa, K., Bleijs, D. A., & Oye, K. A. (2021). Emerging biotechnology and information hazards. *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, 131-140. https://doi.org/10.1007/978-94-024-2086-9

Odetokun, I. A., Jagun-Jubril, A. T., Onoja, B. A., Wungak, Y. S., Raufu, I. A., & Chen, J. C. (2017). Status of laboratory biosafety and biosecurity in veterinary research facilities in Nigeria. *Safety and Health at Work*, *8*(1), 49-58. https://doi.org/10.1016/j.shaw.2016.08.002

Patel, A. U., Williams, C. L., Hart, S. N., Garcia, C. A., Durant, T. J., Cornish, T. C., & McClintock, D. S. (2023). Cybersecurity and information assurance for the clinical laboratory. *The Journal of Applied Laboratory Medicine*, *8*(1), 145-161. https://doi.org/10.1093/jalm/jfac119

Peng, H., Bilal, M., & Iqbal, H. M. (2018). Improved biosafety and biosecurity measures and/or strategies to tackle laboratory-acquired infections and related risks. *International Journal of Environmental Research and Public Health*, *15*(12), 2697. https://doi.org/10.3390/ijerph15122697

Perkins, D., Danskin, K., Rowe, A. E., & Livinski, A. A. (2019). The culture of biosafety, biosecurity, and responsible conduct in the life sciences: a comprehensive literature review. *Applied Biosafety*, *24*(1), 34-45. https://www.liebertpub.com/doi/full/10.1177/1535676018778538

Rathjen, N. A., & Shahbodaghi, S. D. (2021). Bioterrorism. *American Family Physician*, *104*(4), 376-385. https://www.aafp.org/pubs/afp/issues/2021/1000/p376.html

Reardon, S. (2014). Forgotten NIH smallpox virus languishes on death row. *Nature*, *514*(7524), 544. https://doi.org/10.1038/514544a

Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity Implications for the Laboratory of the Future. *Frontiers in Bioengineering and Biotechnology*, *7*, 182. https://doi.org/10.3389/fbioe.2019.00182

Schabacker, D. S., Levy, L. A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Frontiers in Bioengineering and Biotechnology*, *7*, 61. https://doi.org/10.3389/fbioe.2019.00061

Sheldon, J., Ross, S., Morris, T., Brown, I., Zhu, F., Pape, P., & Whitlow, P. (2024). Genomics Cybersecurity Concerns, Challenges, and a Modular Test Lab. In *Proceedings of the 2024 ACM Southeast Conference,* 86-94. https://doi.org/10.1145/3603287.3651215

Subariyah, R., Mantoro, T., & Ratmono, B. M. (2023). The Role of Biosafety and Biosecurity in Biotechnology to Prevent Bioterrorism Threats. In *2023 International Conference on Technology, Engineering, and Computing Applications (ICTECA),* 1-6. https://doi.org/10.1109/ICTECA60133.2023.10490970

Sun, T., Song, J., Wang, M., Zhao, C., & Zhang, W. (2022). Challenges and recent progress in the governance of biosecurity risks in the era of synthetic biology. *Journal of Biosafety and Biosecurity*, *4*(1), 59-67. https://doi.org/10.1016/j.jobb.2022.02.002

Trump, B. D., Galaitsi, S. E., Appleton, E., Bleijs, D. A., Florin, M. V., Gollihar, J. D., & Linkov, I. (2020). Building biosecurity for synthetic biology. *Molecular systems biology*, *16*(7), e9723. https://doi.org/10.15252/msb.20209723

Trump, B. D., Keisler, J. M., Volk, K. M., & Linkov, I. (2020). Biosecurity demands resilience. 4706-4708. https://dx.doi.org/10.1021/acs.est.0c00607?ref=pdf

Vakhter, V., Soysal, B., Schaumont, P., & Guler, U. (2022). Threat modeling and risk analysis for miniaturized wireless biomedical devices. *IEEE Internet of Things Journal*, *9*(15), 13338-13352. https://doi.org/10.1109/JIOT.2022.3144130

Van Puyvelde, S., Deborggraeve, S., & Jacobs, J. (2018). Why the antibiotic resistance crisis requires a One Health approach. *The Lancet Infectious Diseases*, *18*(2), 132-134. https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(17)30704-1/abstract

Wagar, E. (2016). Bioterrorism and the role of the clinical microbiology laboratory. *Clinical Microbiology Reviews*, *29*(1), 175-189. https://doi.org/10.1128/cmr.00033-15

Wang, F., & Zhang, W. (2019). Synthetic biology: recent progress, biosafety and biosecurity concerns, and possible solutions. *Journal of Biosafety and Biosecurity*, *1*(1), 22-30. https://doi.org/10.1016/j.jobb.2018.12.003

Wang, L., Song, J., & Zhang, W. (2021). Journal of Biosafety and Biosecurity. *Tianjin biosecurity guidelines for codes of conduct for scientists: Promoting Responsible Sciences and Strengthening Biosecurity Governance*, *3*, 82-83. https://doi.org/10.1016/j.jobb.2021.08.001

Wani, A. K., Akhtar, N., Sena, S., & Singh, J. (2022). Microbial forensics: A potential tool for investigation and response to bioterrorism. *Health Sciences Review*, *5. 100068*. https://doi.org/10.1016/j.hsr.2022.100068

West, R. M., & Gronvall, G. K. (2020). CRISPR cautions: Biosecurity implications of gene editing. *Perspectives in biology and medicine*, *63*(1), 73-92. https://doi.org/10.1353/pbm.2020.0006

Yin, H., Song, C. Q., Suresh, S., Kwan, S. Y., Wu, Q., Walsh, S., & Anderson, D. G. (2018). Partial DNA-guided Cas9 enables genome editing with reduced off-target activity. *Nature Chemical Biology*, *14*(3), 311-316. https://doi.org/10.1038/nchembio.2559

Zhang, Q., Xing, H. L., Wang, Z. P., Zhang, H. Y., Yang, F., Wang, X. C., & Chen, Q. J. (2018). Potential high-frequency off-target mutagenesis induced by CRISPR/Cas9 in Arabidopsis and its prevention. *Plant Molecular Biology*, *96*, 445-456. https://doi.org/10.1007/s11103-018-0709-x

Zhou, D., Song, H., Wang, J., Li, Z., Xu, S., Ji, X., & Xu, J. (2019). Biosafety and biosecurity. *Journal of Biosafety and Biosecurity*, *1*(1), 15-18. https://doi.org/10.1016/j.jobb.2019.01.001