frontiers in Bioengineering and Biotechnology

PERSPECTIVE
published: 06 June 2019
doi: 10.3389/fbioe.2019.00099

Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape

Lauren C. Richardson[1]*, *Nancy D. Connell*[2], *Stephen M. Lewis*[1], *Eleonore Pauwels*[3] and *Randy S. Murch*[4]

[1] Merrick & Co., Arlington, VA, United States, [2] Johns Hopkins Center for Health Security, Bloomberg School of Public Health, Baltimore, MD, United States, [3] Wilson Center Science and Technology Innovation Program, The Wilson Center, Washington, DC, United States, [4] Virginia Tech Research Center, School of Public and International Affairs, Virginia Polytechnic Institute and State University, Arlington, VA, United States

OPEN ACCESS

Edited by:
Stephen Allen Morse, Centers for Disease Control and Prevention (CDC), United States

Reviewed by:
Dana Perkins, United States Department of Health and Human Services, United States
Laura Adam, Ebiosec, Inc, United States

***Correspondence:**
Lauren C. Richardson
Lauren.Richardson@merrick.com

Specialty section:
This article was submitted to Biosafety and Biosecurity, a section of the journal Frontiers in Bioengineering and Biotechnology

Received: 30 January 2019
Accepted: 18 April 2019
Published: 06 June 2019

Citation:
Richardson LC, Connell ND, Lewis SM, Pauwels E and Murch RS (2019) Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape. Front. Bioeng. Biotechnol. 7:99. doi: 10.3389/fbioe.2019.00099

The life sciences now interface broadly with information technology (IT) and cybersecurity. This convergence is a key driver in the explosion of biotechnology research and its industrial applications in health care, agriculture, manufacturing, automation, artificial intelligence, and synthetic biology. As the information and handling mechanisms for biological materials have become increasingly digitized, many market sectors are now vulnerable to threats at the digital interface. This growing landscape will be addressed by cyberbiosecurity, the emerging field at the convergence of both the life sciences and IT disciplines. This manuscript summarizes the current cyberbiosecurity landscape, identifies existing vulnerabilities, and calls for formalized collaboration across a swath of disciplines to develop frameworks for early response systems to anticipate, identify, and mitigate threats in this emerging domain.

Keywords: biosecurity, cybersecurity, cyberbiosecurity, life sciences, bioeconomy, bioinformatics, synthetic biology, biomanufacturing

INTRODUCTION

The greatest vulnerabilities in any field can be found at its margins—at its junctions with adjacent fields. The new discipline of cyberbiosecurity has been created to bring together disparate communities to identify and address a complex ecosystem of security vulnerabilities at the interface of the life sciences, information systems, biosecurity, and cybersecurity (Murch et al., 2018; Peccoud et al., 2018); it serves as a lens for observation that relies on disciplinary integration. Cyberbiosecurity describes an intersection of disciplines that falls outside any single sector; because these convergences are not clearly analyzed, actors within a single sector do not have agency to address potential issues and are less likely to cooperate. Such vulnerabilities exist within biomanufacturing, cyber-enabled laboratory instrumentation and patient-focused systems, "Big Data" generated from "omics" studies, and throughout the farm-to-table enterprise (**Figure 1**). In addition to fundamental and applied research and development opportunities, off-the-shelf solutions not yet applied in this domain likely exist. While the term is new, the concept of

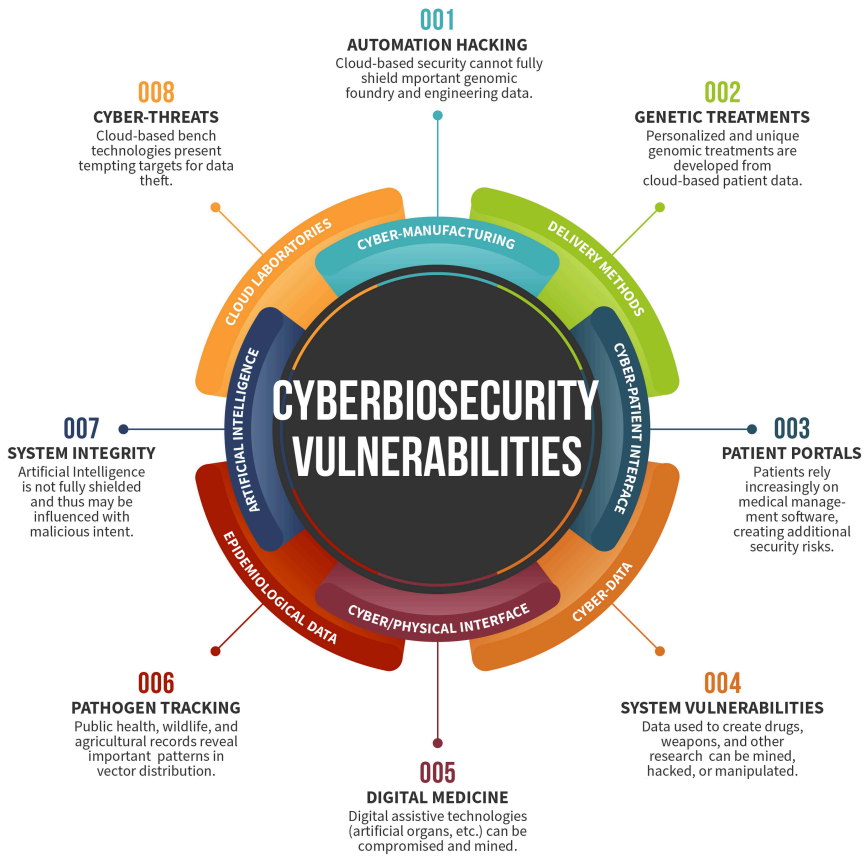

FIGURE 1 | Summary of cyberbiosecurity vulnerabilities across the spectrum of the bioeconomy. Each sector of the wheel describes specific vulnerabilities that span the medicine, infectious disease, systems management, and biotechnology.

cyberbiosecurity has been acknowledged as a serious concern (Wintle et al., 2017). The issues raised in the area of cyberbiosecurity will have substantial impact on the growing bioeconomy[1].

The solution set is not simply technical: creating cross-sector convergence opportunities for effective communication and collaboration as well as governance, policy, and regulatory structures is also necessary. Derived value from cyberbiosecurity endeavors potentially embraces economic impact, national security, societal resilience, and environmental sustainment. In this paper, we establish a landscape for cyberbiosecurity and issue a call for cooperation across sectors to recognize and mitigate potential threats.

BACKGROUND

As a part of the discussion, we refine the definition of cyberbiosecurity. **Cybersecurity** encompasses the protection of computer systems from theft and damage to their hardware, software, or information, as well as from disruption or misdirection of the services they provide. **Biosecurity** involves securing valuable biological material from misuse or harm. Initially, Murch et al. defined cyberbiosecurity as the "developing understanding of the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life science, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate, and attribute such threats as it pertains to security, competitiveness, and resilience" (Murch et al., 2018). The definitions of cybersecurity and biosecurity both include an underlying assumption of value on the part of the material in question. We further suggest expansion of this definition of cyberbiosecurity to differentiate it from the individual scopes of cybersecurity and biosecurity. Cyberbiosecurity addresses the potential for or actual malicious destruction, misuse, or exploitation of valuable information, processes, and material at the interface of the life sciences and digital worlds; concept mastery requires an understanding of this interface in the context of the threat of malignant use of technology in general. This paper is a call to action before such a succession of events takes place.

[1]Bioeconomy is defined as "economic activity that is fueled by research and innovation in the biological sciences (House, 2012)."

LANDSCAPE

Cyberbiosecurity cuts across disciplines; impacting fields from laboratory science, to human and animal health, agriculture, and environmental health and ranging from protection to management and remediation. Technology integration is the new norm, with novel technology improvements and simple digitization bringing easy access to old systems, such as medical records. As technical disciplines develop at an exponential pace and their convergence accelerates, it is becoming increasingly clear that the fields of cybersecurity and biosecurity must also converge in order to address inherent digital and biological concerns. Further, technological convergence meets the decreasing cost for access at the Do It Yourself (DIY)/community biology space.

CYBERBIOSECURITY IN BIOTECHNOLOGY

Artificial Intelligence

Industry interest in artificial intelligence (AI) has experienced a resurgence in recent years due to increased computing power, advancing applications of neural networks, and an emergence of new machine and deep learning techniques across the biology sector. Biotechnology companies are successfully utilizing these developments for drug design and development (Zilinskas, 2017), genomics (Pauwels and Vidyarthi, 2017), evolutionary biology (Feltes et al., 2018), protein folding (Paladino et al., 2017), and more. This rapid and evolving interest in the landscape of new AI technologies has led to emerging threat domains related to information privacy and storage, ownership over biological and genetic data, and applications of powerful technologies (Pauwels, 2018). These issues are not new, as bioinformatics and digitization have created a potential target; however, the popularization of AI has refreshed these concerns in the modern zeitgeist. There is a renewed opportunity for life science and cybersecurity professionals to design and implement frameworks to facilitate responsible application of AI techniques to biology.

Automation

The convergence of robotics, machine learning, and artificial intelligence has paved the way for automated approaches to biology, manufacturing, software development, accounting, and more. Improved biological engineering techniques and robotics have converged to result in rapid prototyping and higher yields. Laboratories are increasingly using robots to improve throughput and free up the hands of laboratorians around the world (McGee, 2014; Szesterniak, 2014). As robots are increasingly connected to networks and other electronic systems, new cyberbiosecurity concerns unique to automated laboratory environments are beginning to emerge. Virtual environments allow access to infrastructure within the physical world; this creates a vulnerability that would permit unauthorized remote access to an automated biological manufacturing system. As automation increases within the life sciences, so too will potential vulnerabilities to threat.

Synthetic Biology

The term "synthetic biology" is widely used to describe activities carried out by scientists in a variety of disciplines, from bioengineering, chemistry, biochemistry, and materials science to cellular and molecular biology (Hobom, 1980; Purnick and Weiss, 2009). Today, engineers, biologists, technologists, and citizen scientists have turned this field into a true discipline. Systems engineering techniques are being applied to organisms to design genetic circuits, novel molecules, and commodities such as fuels, electricity, feed, and renewable materials (Rollin et al., 2013; Kiss et al., 2014). Simultaneously, the design-build-test approach traditionally used in product development is rapidly emerging in organism engineering (Dudley et al., 2015; Gill et al., 2016). Advancements in synthetic biology will have a significant impact on cyberbiosecurity as laboratory automation techniques become more widespread and the traditional cost barrier for scale-up of production is lowered. Similarly, the convergence of robotics, microfluidics, cell-free systems design and synthetic metabolic engineering stands to create new cyberbiosecurity risks and unique threat domains (Nielsen and Keasling, 2011; Murch et al., 2018; Peccoud et al., 2018). As these fields further develop and converge, revealed vulnerabilities will offer new opportunity for exploitation.

CYBERBIOSECURITY IN DIGITIZATION OF TRADITIONAL TECHNOLOGY

Manufacturing

Science and technology-reliant organizations are becoming more complex and networked throughout facilities, supply chains, logistics, and transport mechanisms. Distributed manufacturing employs decentralized production networks linked by information technology; as more connections between traditionally isolated systems are developed, more security controls must be considered in order to mitigate risks and reduce vulnerabilities. The production processes and assemblies of biologics and other materials can also be distributed and carried out asynchronously at geographically different locations, allowing response to potential threats to be developed *in situ*.

In addition to facilitation of distributed manufacturing techniques for traditional life sciences operations, recent advances in cell-free metabolic engineering technologies allow for higher throughput in production environments. This has resulted in improved biological techniques for rapid prototyping and higher yields. Cell-free biological systems are being used to develop commodities such as fuels, electricity, feed, and renewable materials (Rollin et al., 2013). As the convergence of dichotomous technical disciplines (e.g., automation and cellular biology) continues to expand rapidly, it is increasingly important that the fields of cybersecurity and biosecurity converge to address inherent digital and biological concerns.

Biomedical Sciences

Cybersecurity and health security converge with increasing digitization of health data. Regulatory mechanisms are in place to address concerns regarding privacy and confidentiality of medical and billing information; however, this extends beyond the cyber-patient interface in the context of electronic medical records. Patient treatment management—including potential drug interactions, protocols, and sensitivities specific to the patient—is increasingly digitized. Personalized medicine diagnostics and therapeutics are rapidly expanding, and much of the information associated with these interventions is maintained digitally. Biomedical data breaches are not without historic precedent: in 2014, data breaches of three major health systems resulted in unauthorized access to millions of patient records, including clinical data (Kozminski, 2015). These breaches provided the perpetrators valuable clinical data, which could be used internally or sold for monetary gain. In addition to facilitating illicit data collection, disruption of digitally-programmed diagnostic testing systems or therapeutic targeting fields could result in ineffective treatment. Medical devices are also an area of interest in cyberbiosecurity, as many potential exploits could be leveraged through direct and indirect interfaces with the patient and manufacturer (Khera, 2017).

Agriculture

Throughout much of the world, food and beverage safety and security is a high priority. Concomitantly, the economics, societal robustness, and security implications of agriculture, foodstuffs and beverages are massive. Extensive quality measures are in place to prevent and mitigate threats from manifesting; outbreak and contamination detection and response systems react when problems are noticed. Packaging and labeling methodology have also been improved. However, agriculture and consumables in many countries rely on cyber-enabled systems for many aspects of farm management, production-to-consumption, raw materials to finished product, and logistics (Security Security DoH., 2018). The health and security of this dimension of agriculture and food systems is unclear from a cyberbiosecurity perspective. We reason that vulnerable critical links and nodes exist throughout this highly complex global and national ecosystem; attention to cyberbiosecurity measures is warranted and would be considerably beneficial.

CONCLUSION

The convergence of recent advances in the life sciences with regard to traditional cybersecurity threats has led to the recognition and identification of vulnerabilities, known as cyberbiosecurity threats (Murch et al., 2018; Peccoud et al., 2018). Here we present a preliminary review of the landscape of these threats and propose recommendations to activate a "call to action" to anticipate these threats and mitigate their effects. Several entities have approached related issues: for example, in October 2019, HHS announced the opening of the Health Sector Cybersecurity Coordination Center (HC3), intended to prevent threats to health data through strengthening cybersecurity (Office Office HP., 2018). Though concurrent efforts touch on the issues described, individual efforts alone are insufficient to cover the breadth of the landscape. We call for analyses and publications to fully scope cyberbiosecurity and identify a comprehensive strategy to establish the discipline's goals and objectives; we call for carefully-crafted national or international meetings of experts from appropriate science, technology, and social science domains to begin to bring communities together to define priorities for approaches to solutions by examining causes, effects and possible remedies; we call for initiation of campaigns of blended teams of experts engaging key government agencies to raise awareness and initiate creation of and/or changes to relevant policies and programs in order to incorporate relevant cyberbiosecurity perspectives.

AUTHOR CONTRIBUTIONS

LR, NC, SL, EP, and RM contributed conception and design of the manuscript. LR, NC, SL, and RM wrote sections of the manuscript. All authors contributed to manuscript revision, read, and approved the submitted version.

ACKNOWLEDGMENTS

The authors acknowledge the graphic talents of LJ DeGraffenreid.

REFERENCES

Dudley, Q. M., Karim, A. S., and Jewett, M. C. (2015). Cell-free metabolic engineering: biomanufacturing beyond the cell. *Biotechnol. J.* 10, 69–82. doi: 10.1002/biot.201400330

Feltes, B. C., Grisci, B. I., Poloni, J. F., and Dorn, M. (2018). Perspectives and applications of machine learning for evolutionary developmental biology. *Mol. Omics* 14, 289–306. doi: 10.1039/C8MO00111A

Gill, R. T., Halweg-Edwards, A. L., Clauset, A., Way, S. F., et al. (2016). Synthesis aided design: the biological design-build-test engineering paradigm? *Biotechnol. Bioeng.* 113, 7–10. doi: 10.1002/bit.25857

Hobom, B. (1980). Gene surgery: on the threshold of synthetic biology. Med. *Klin.* 75, 834–841.

House, T. W. (2012). National bioeconomy blueprint, April 2012. *Industrial Biotechnol.* 8, 97–102. doi: 10.1089/ind.2012.1524

Khera, M. (2017). Think like a hacker: insights on the latest attack vectors (and security controls) for medical device applications. *J. Diabetes Sci. Technol.* 11, 207–212. doi: 10.1177/1932296816677576

Kiss, A. A., Grievink, J., and Rito-Palomares, M. (2014). A systems engineering perspective on process integration in industrial biotechnology. *J. Chem. Tech. Biotech.* 90, 349–355. doi: 10.1002/jctb.4584

Kozminski, K. G. (2015). Biosecurity in the age of Big Data: a conversation with the FBI. *Mol. Biol. Cell* 26, 3894–3897. doi: 10.1091/mbc.E14-01-0027

McGee, J. (2014). Screening Robotics and Automation. *SLAS Discov. Adv. Life Sci.* 19, 1131–1132. doi: 10.1177/1087057114538231

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., and Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. *Front. Bioeng. Biotechnol.* 6:39. doi: 10.3389/fbioe.2018.00039

Nielsen, J. K., and Keasling, J. D. (2011). Synergies between synthetic biology and metabolic engineering. *Nat. Biotechnol.* 29, 693–695. doi: 10.1038/nbt.1937

Office HP. (2018). *HHS Announces the Official Opening of the Health Sector Cybersecurity Coordination Center*. U.S. Department of Health & Human Services: HHS.gov.

Paladino, A., Marchetti, F., Rinaldi, S., and Colombo, G. (2017). Protein design: from computer models to artificial intelligence. *WIREs Comput. Mol. Sci.* 7:e1318. doi: 10.1002/wcms.1318

Pauwels, E. (2018). *The Ethical Anatomy of Artifical Intelligence*. New York, NY: U.N. University.

Pauwels, E., and Vidyarthi, A. (2017). *Who Will Own the Secrets in Our Genes? A US-China Race in Artificial Intelligence and Genomics*. Washington, DC: Woodrow Wilson International Center for Scholars.

Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., and Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. *Trends Biotechnol.* 36, 4–7. doi: 10.1016/j.tibtech.2017.10.012

Purnick, P. E., and Weiss, R. (2009). The second wave of synthetic biology: from modules to systems. *Nat. Rev. Mol. Cell Biol.* 10, 410–422. doi: 10.1038/nrm2698

Rollin, J. A., Tam, T. K., and Zhang, Y. H. P. (2013). New biotechnology paradigm: cell-free biosystems for biomanufacturing. *Green Chem.* 15, 1708–1719. doi: 10.1039/c3gc40625c

Security DoH. (2018). *Threats to Precison Agriculture*.

Szesterniak, M. (2014). Six *Trends in Robotics in the Life Sciences*. Available online at: http://www.parkermotion.com/whitepages/Six-Trends-in-Life-Science-Robotics.pdf

Wintle, B. C., Boehm, C. R., Rhodes, C., Molloy, J. C., Millett, P., Adam, L., et al. (2017). Point of view: a transatlantic perspective on 20 emerging issues in biological engineering. *Elife* 2017:e30247. doi: 10.7554/eLife.30247

Zilinskas, R. A. (2017). A brief history of biological weapons programmes and the use of animal pathogens as biological warfare agents. *Rev. Sci. Tech.* 36, 415–422. doi: 10.20506/rst.36.2.2662

Conflict of Interest Statement: LR and SL were employed by Merrick and Company.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.