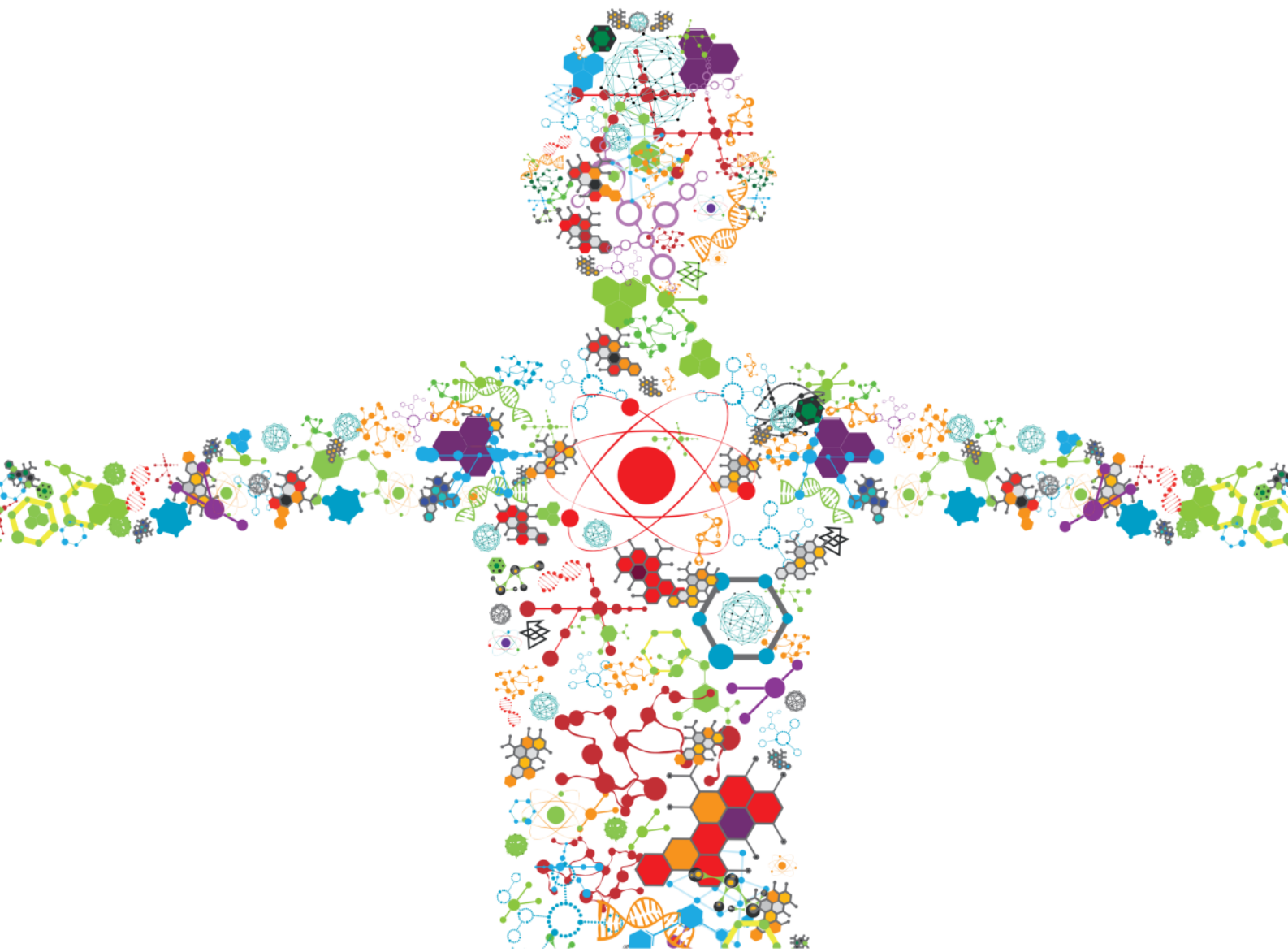
MAPPING THE CYBERBIOSECURITY ENTERPRISE

EDITED BY: Randall Murch and Diane DiEuliis
PUBLISHED IN: Frontiers in Bioengineering and Biotechnology



frontiers Research Topics

frontiers

ISSN 1664-8714
ISBN 978-2-88963-213-8
DOI 10.3389/978-2-88963-213-8

About Frontiers

Frontiers is more than just an open-access publisher of scholarly articles: it is a pioneering approach to the world of academia, radically improving the way scholarly research is managed. The grand vision of Frontiers is a world where all people have an equal opportunity to seek, share and generate knowledge. Frontiers provides immediate and permanent online open access to all its publications, but this alone is not enough to realize our grand goals.

Frontiers Journal Series

The Frontiers Journal Series is a multi-tier and interdisciplinary set of open-access, online journals, promising a paradigm shift from the current review, selection and dissemination processes in academic publishing. All Frontiers journals are driven by researchers for researchers; therefore, they constitute a service to the scholarly community. At the same time, the Frontiers Journal Series operates on a revolutionary invention, the tiered publishing system, initially addressing specific communities of scholars, and gradually climbing up to broader public understanding, thus serving the interests of the lay society, too.

Dedication to Quality

Each Frontiers article is a landmark of the highest quality, thanks to genuinely collaborative interactions between authors and review editors, who include some of the world's best academicians. Research must be certified by peers before entering a stream of knowledge that may eventually reach the public - and shape society; therefore, Frontiers only applies the most rigorous and unbiased reviews.
Frontiers revolutionizes research publishing by freely delivering the most outstanding research, evaluated with no bias from both the academic and social point of view. By applying the most advanced information technologies, Frontiers is catapulting scholarly publishing into a new generation.

What are Frontiers Research Topics?

Frontiers Research Topics are very popular trademarks of the Frontiers Journals Series: they are collections of at least ten articles, all centered on a particular subject. With their unique mix of varied contributions from Original Research to Review Articles, Frontiers Research Topics unify the most influential researchers, the latest key findings and historical advances in a hot research area! Find out more on how to host your own Frontiers Research Topic or contribute to one as an author by contacting the Frontiers Editorial Office: researchtopics@frontiersin.org

Table of Contents

frontiers in Bioengineering and Biotechnology

EDITORIAL
published: 03 October 2019
doi: 10.3389/fbioe.2019.00235

Editorial: Mapping the Cyberbiosecurity Enterprise

Randall Murch[1*†] *and Diane DiEuliis*[2†]

[1] Virginia Tech, Blacksburg, VA, United States, [2] National Defense University, Washington, DC, United States

Keywords: cyberbiosecurity, bioeconomy, biosecurity, national security, biotechnology

Editorial on the Research Topic

Mapping the Cyberbiosecurity Enterprise

We are pleased to introduce this Research Topic in Frontiers in Bioengineering and Biotechnology on a new area of biosecurity, termed "Cyberbiosecurity." This term, originally introduced in the recently published strategic article by Murch et al. entitled "Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy (*Front. Bioeng. Biotechnol.* doi: 10.3389/fbioe.2018.00039), describes the security vulnerabilities that exist at the intersection of cybersecurity, cyber-physical security, and biosecurity.

Entitled "*Mapping the Cyberbiosecurity Enterprise,*" this collective of papers was amassed to firmly establish this topic as a new discipline within biosecurity. Each article contributes to developing and presenting deeper understanding of this emerging topic, and helps to delineate the range of current and potential applications of cyberbiosecurity. We also anticipate that this collective will foster greater engagement between the biosecurity and cybersecurity communities.

"Cyberbiosecurity" has been defined as "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, 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." While cybersecurity is a broad and well-researched existing field, its application to specific aspects of the life sciences necessitates a conjoining of experts from each discipline which have predominantly existed in silos to date. Defining cyberbiosecurity as a discipline is a necessary first step in bringing these disparate groups together to expand understanding of the risks from their relative perspectives.

Mapping the topology of cyberbiosecurity has just begun, but proponents have realized that it has expansive applications across the life sciences, most obviously in the biomedical and pharmaceutical domains. But as the digitization of biology grows, biotechnology is expanding far beyond these traditional silos. The purposeful engineering of biology, including application of the classical "design, build, test" cycle, is opening unprecedented opportunities for biomaterials and biofuels and their use, for agriculture and food systems (from large scale crop engineering to "farm to table"), and for bioinformatics and "AI" (from small field tools to large-scale complex systems and cloud computing). As biotechnologies continue to advance and evolve, cyberbiosecurity will be a key consideration in existing critical infrastructure related to all these arenas. Further, new components of critical infrastructure may emerge and be defined through advances in the synthetic biology industry, and cybersecurity will need to be assessed for those new components. In our view, awareness and identification of vulnerabilities is an important first step in launching the field, followed by the development and implementation of mitigations and solutions. Eventually, practitioners in this growing field will be responsible for the development of guidelines and standards of governance, which will require adherence and compatibility with existing national defense strategies.

OPEN ACCESS

Edited and reviewed by:
Kenneth I. Berns,
University of Florida, United States

***Correspondence:**
Randall Murch
rmurch@vt.edu

[†] These authors have contributed equally to this work

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

Received: *30 August 2019*
Accepted: *10 September 2019*
Published: *03 October 2019*

Citation:
Murch R and DiEuliis D (2019) Editorial: Mapping the Cyberbiosecurity Enterprise. Front. Bioeng. Biotechnol. 7:235. doi: 10.3389/fbioe.2019.00235

This Special Collection, represented by both U.S. and international contributors, includes writings on a number of the topical areas described above. Vulnerabilities associated with synthetic biological manufacturing are described, including specific discussions of biopharmaceutical production. The evolving platforms for biotechnology, including distributed manufacturing models and laboratory automation, are included for consideration. Importantly, a discussion of the public health and stability ramifications of cyberbiosecurity in settings outside the US are also considered. General themes in other fields, such as agriculture, biopharma, and labs of the future are represented in stand-alone contributions. Some technical aspects of tool development, such as DNA synthesis security screens, and access to pathogen genome databases provide insights on current thinking and perceptions of risk. Finally, broad consideration is given to cyberbiosecurity in the national security context, given any new aspect of biosecurity must mesh with existing national security approaches and frameworks in the biodefense realm. Authors have also provided discussions of options for training and strategies for workforce development, all of which can help to build not only a general awareness of cybersecurity among biologists and synthetic biology engineers, but potentially develop a core of cyberbiosecurity specialists or practitioners that will be needed for risk assessments and solutions.

It is our hope that this eclectic set of insights and perspectives will broadly stimulate academia, government, non-profits, and the private sector to identify, prioritize, resource and pursue research, and implement solutions in the realm of cyberbiosecurity. Such research, outcomes and change management should focus on risk analysis, methods and technologies, education and training, guidelines and standards, policy, regulations and legal frameworks.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

Conflict of Interest: The 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.

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

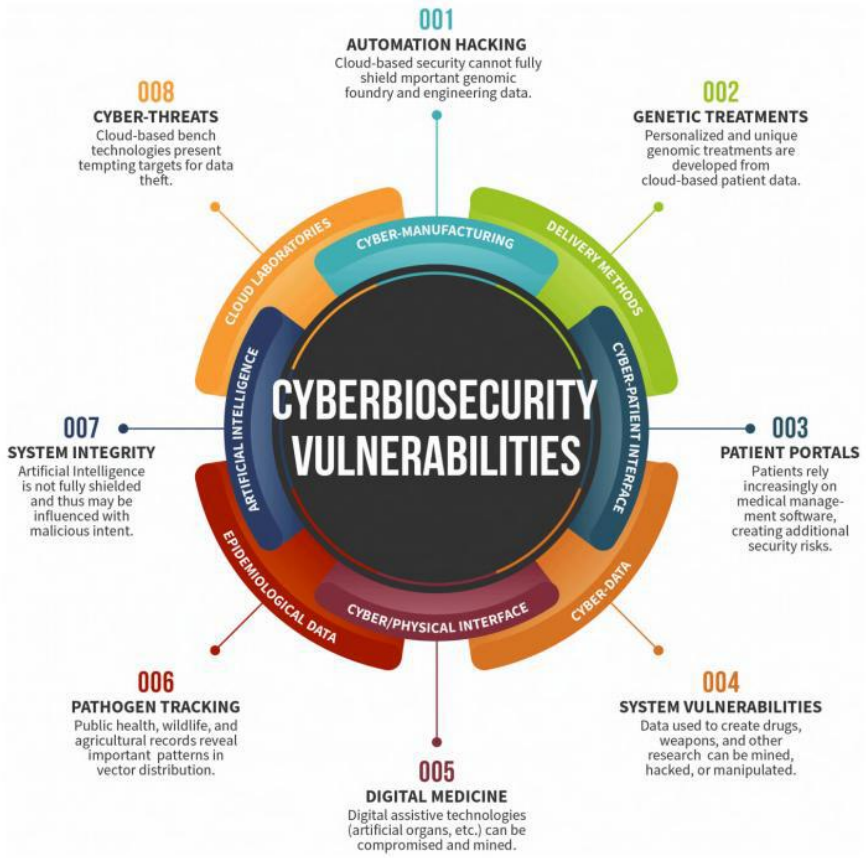


FIGURE 1 | Summary of cyberbiosecurity vulnerabilities across the spectrum of the bioeconomy. Each sector of the wheel describes specific vulnerabilities that span the medicine, infectious disease, systems management, and biotechnology.

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.

frontiers in Bioengineering and Biotechnology

BRIEF RESEARCH REPORT
published: 19 June 2019
doi: 10.3389/fbioe.2019.00136

Cyber-Biosecurity Risk Perceptions in the Biotech Sector

Kathryn Millett, Eduardo dos Santos and Piers D. Millett*

Biosecure Ltd, Market Rasen, United Kingdom

The expanding digitization of the biological sciences places greater value on the data generated, information extrapolated and knowledge gained. Failing to protect data will affect a company or country's ability to position itself optimally in the forthcoming fourth industrial revolution. Further, more reliance on automation, distribution, and outsourcing in biotechnology makes its infrastructure a target. The equipment and service providers that drive physical research and development are also all connected online. Failing to protect these resources from intrusion increases the risk of accidental or deliberate harm, for example by the loss of control over biological products. Robust cybersecurity measures are therefore critical for both securing the data generated by the biotechnology sector as well as securing key infrastructure. Cyber-biosecurity is emerging multidisciplinary field that combines cybersecurity, biosecurity, and cyber-physical security as relates to biological systems (Murch et al., 2018). To better identify the perceived risks at the interface between cybersecurity and biosecurity, Biosecure conducted a pilot study that surveyed the opinions of a discrete set of international field leaders in biotechnology and cybersecurity. The survey was carried out online from October-November 2017. Key findings of the survey showed that cyber-biosecurity risks were considered to be difficult to characterize due to variations in types of threats, targets and potential impacts, and compounded by a notable variation between the level of sophistication or maturity of mitigation and response measures. Further research is therefore necessary bringing together the different communities focusing on these issues to develop a common language, better define the threats and discuss potential ways forward in addressing risks.

Keywords: cyber-biosecurity, biotechnology, bioeconomy, infrastructure, risk perception, biosecurity, industry

OPEN ACCESS

Edited by:
Diane DiEuliis, National Defense University, United States

Reviewed by:
Gregory D. Koblentz, George Mason University, United States
Dana Perkins, United States Department of Health and Human Services, United States

****Correspondence:***
Kathryn Millett
kathryn@biosecu.re

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

Received: *26 November 2018*
Accepted: *21 May 2019*
Published: *19 June 2019*

Citation:
Millett K, dos Santos E and Millett PD (2019) Cyber-Biosecurity Risk Perceptions in the Biotech Sector. Front. Bioeng. Biotechnol. 7:136. doi: 10.3389/fbioe.2019.00136

INTRODUCTION

The development and recognition of "cyber-biosecurity" as an important element in securing data and products emerging from the biotechnology and biomedical sectors has predominantly emerged from the field of biosecurity. While the risks relating to accessing private biomedical data and the theft of valuable data from an intellectual property standpoint are well-known and recognized, the biosecurity implications of cyber intrusions relating to biotechnology infrastructure remain largely unknown in commercial biotechnology facilities.

To better gauge the current level of understanding and awareness of cyber-biosecurity risks in the biotechnology sector and identify how the risks are perceived, Biosecure conducted a pilot survey targeting a discrete set of international leaders in the fields of biotechnology and cybersecurity.

METHODOLOGY

To conduct a discrete pilot survey of the types and level of cyber-biosecurity risks identified in the field of biotechnology, a short questionnaire comprising 12 questions that was posted securely online. The questions posed were a mix of multiple choice and open-ended questions, divided across the themes of risk perception and awareness, risk mitigation capacities and resources, and the urgency of, and potential avenues for, any future action. The questions were reviewed by an expert in qualitative methodology to eliminate any issues of bias.

The survey described in this paper was conducted in accordance with the Declaration of Helsinki and all participants provided informed consent in writing (World Medical Association, 2013). The survey described is not considered research by the UK National Health Service and Medical Research Council and does not require review by a Research Ethics Committee. In addition, Biosecure Ltd. funded the survey using its own corporate funds. Biosecure Ltd. does not, and has not, received US Federal research funding. As a result, the survey described in this paper was performed in accordance with relevant institutional and national guidelines.

Twenty-six individuals were invited to participate from across the biotech and cybersecurity sector. Invitees from the biotech sector included founders of small to medium biotechnology companies in the United States and United Kingdom, senior management of large biotechnology companies (with an international footprint), representatives of industry, venture capitalists specializing in biotechnology, and advisors to the above on security issues. The individuals approached in the cybersecurity sector included industry specialists, leading academics, national government experts, experts in leading think tanks, and specialists within intergovernmental organizations.

Overall, of the 26 invited questionnaire participants, 13 agreed to participate. The responses were anonymized.

SURVEY RESULTS

The results of the survey were assessed according to four key areas: (1) assessing the threat; (2) assessing threat mitigation and response capacity; (3) available tools and resources; and, (4) recommended next steps. The key findings under each of these areas are elaborated below and summarized in **Table 1**.

Assessing the Threat

Over two-thirds of respondents deemed the risks posed to the biotechnology sector by cyber threats and intrusions as elevated or severe when compared to normal operating standards in the biotech industry. The two scenarios perceived to pose the greatest risk were: unauthorized access to data, information, or knowledge outside the public domain; and unauthorized actors able to secretly change data, information, or knowledge. In only one scenario (in which an unauthorized actor takes control of infrastructure) did any respondent think there was no or minimal risk.

- When asked to identify different types of risks from cybersecurity breaches in the biotech sector, participants noted potential negative impacts from:
- The theft, elimination or ransom of data, algorithms, or software with a direct or indirect impact on R&D or commercial operations;
- Modification of data, algorithms, or software with a direct or indirect impact on research and development or commercial operations;
- The loss of intellectual property or commercial advantage by data, algorithms, or software being available to competitors;
- Potential for the disabling or disruption of important systems or infrastructure leading to disruption of commercial operations or impeding good manufacturing practices;
- Manipulation of bio-manufacturing or automated systems to create risks.

Respondents ranked states and proxies used by states as the type of actor posing the greatest risk, with lone individuals viewed as generating the least risk. This survey did not differentiate between insider or outsider threats, regardless of whether states, groups or lone individuals. This may be an area ripe for further study.

All participants considered that cyber-biosecurity risks posed a real and current threat, but that these were not, or only partially, being addressed within the biotech sector. In part, this was considered due to a lack of awareness and information within the biotech community, with one participant noting that "[M]any companies are unaware of the intensity of outsider threats because they are not actively monitoring these activities."

Assessing Current Threat Mitigation and Response Capacities

While noting the lack of sufficient information on the type and level of biorisks to the biotech sector by cyber intrusions, over seventy-five per cent (75%) of participants indicated that their organizations had undertaken some efforts to address cybersecurity issues, and ninety per cent (90%) of these reported that such measures were regularly reviewed.

However, the comprehensiveness and maturity of mitigation efforts were reported as being varied, with some participants reporting that their efforts were only in the nascent stages. One respondent, for example, noted that their activities had been "...mostly discussions that it will be a problem but they have no idea nor urge to address it." Another noted that the issues had been considered "[F]airly deeply, although [we] have not… done any work to implement anything."

By contrast, other participants had begun integrating cybersecurity into their business with a participant reporting that "[W]e have considered security implications in our technology development at all levels… partner technologies we integrate have always required a careful discussion of the security implications that flow from their use, and as a result we rely heavily on technologies from vendors such as Google and Microsoft that have strong security cultures."

In addition to variances in awareness and the perceived risks posed by cyber-attacks to biological facilities and equipment, respondents pinpointed the lack of available resources as a

limiting factor for addressing cyber-biosecurity. Over ninety per cent (90%) of participants expressed a strong view that insufficient time and resources are being dedicated to dealing with these risks. One participant noted they "have not yet had the resources to do formal red team testing of our systems" and another commented that "[S]ufficient time and resources are almost never dedicated to dealing with risks from cybersecurity; biotech is no exception." Further, it was remarked that "[D]ealing with cybersecurity breaches is not a one size fits all process. Filling the gaps on the topic requires a tailored approach for each company, entity, or facility. By performing a comprehensive gap analysis for each entity, the answer to this question can be discovered."

When asked their view on the appropriate agency to take the lead in addressing any risks from cybersecurity breaches in biotechnology, participants showed a wide divergence of opinion (**Figure 1**) suggesting that a multi-stakeholder approach may be warranted.

Available Tools and Resources

Over seventy-five (75%) of respondents were unaware of any dedicated resources (reports, guidance, standards, etc.) for dealing with risks from cybersecurity breaches in biotechnology. Those that were aware of existing resources highlighted internal company resources, broader standards that incorporated aspects of biosecurity and cybersecurity but which did not specifically address the overlap, or country-specific resources, such as National Institute of Standards and Technology and FBI outreach agents in the USA.

However, there was greater awareness (50%) of the existence of "dedicated support for dealing with this issue (such as hotlines, reporting infrastructure, national experts, commercial services,

TABLE 1 | Relative risk perception of different cybersecurity threats to biotech.

	No or minimal risk	Risk comparable to normal operating standards	Elevated or severe risk
An incident in which an unauthorized actor takes control of infrastructure (e.g., lab equipment, lab control systems, or even a fully automated robot lab)	2	2	9
An incident in which an unauthorized actor accesses data, information, or knowledge that is not in the public domain	0	2	11
An incident in which an unauthorized actor is able to circumvent security controls, such as those used to screen orders and customers amongst certain biotech service providers	0	3	9
An incident in which an unauthorized actor is able to secretly change data, information, or knowledge	0	1	12
An incident in which an unauthorized actor is able to interrupt the functioning of lab systems	0	4	9
An incident originating from a compromise in the supply chain	0	2	9

White, No response; Yellow, 1 to 5 responses; Orange, 6 to 10 responses; Red, Over 10 responses.

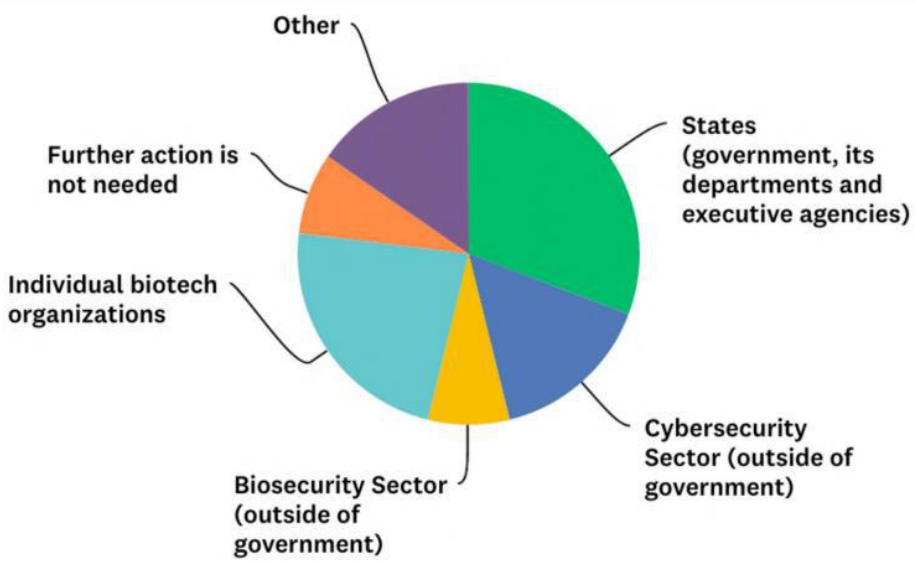


FIGURE 1 | Views as to the appropriate primary actor in addressing any risks from cybersecurity breaches in biotech.

etc." with two thirds of those respondents aware of support citing the Weapons of Mass Destruction (WMD) Directorate of the FBI and one respondent citing private company, Ebiosec. No participant identified sources of support that specifically address the cybersecurity needs of the biotech sector outside of the USA.

Recommended Next Steps in Addressing Cyber-Biosecurity

Several respondents pointed to efforts to address gaps in the interface between cyber- and biosecurity including sponsored meetings and, in a few cases, having specifically allocated staff time to addressing these issues. In addition, notice has been made of the emergence of new actors in the field, including such as companies like Ebiosec which provides services to "manage, model, secure, and visualize their data-driven life sciences operations[1]." The founders of this company also manage an online portal for "fostering discussions and sharing information, events and tools to secure the digital dimension of the biothreat[2]."

However, the majority of participants acknowledged that much more needs to be done to bring together the communities addressing biosecurity and cybersecurity, and identify effective measures and approaches to mitigate and prevent the risks, including fine tuning broader regulatory approaches to help foster a cybersecurity culture. One participant noted "Biotech does not think about security other than more traditional biosecurity and biosafety; security communities do not understand biotech (focused on traditional telecoms and digital)."

[1]See http://ebiosec.com/

[2]See http://information-biosecurity.org/

A number of issues warranting increased attention were also identified, including: the implications of new supply/value chains; techno-espionage or potential for business model/regulatory disruptions; loss of public/political trust resulting from inactivity; and how cybersecurity risk impacts competitiveness of biotechnology companies.

CONCLUSION

The issue of cyber-biosecurity is not well-known or understood, even among biotechnology and cybersecurity experts. A concerted effort to develop this emerging field, define, and foster awareness of the threats and craft a common language is therefore a pressing need as the digital age of biology progresses.

Opportunities are needed to bring together communities focusing on these issues, and begin work on areas of common interest and the means to address the identified risks. Strengthened multi-stakeholder capacity is needed to work at the interface between cybersecurity and biosecurity, and support and resources should be invested in further understanding cybersecurity risks in the biotechnology sector in order to develop appropriate counter measures.

AUTHOR CONTRIBUTIONS

KM is the lead author of this paper. PM and KM devised and carried out the survey. EdS provided technical assistance during the survey and conducted a literature review on cyberbiosecurity.

REFERENCES

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

World Medical Association (2013). *Declaration of Helsinki Ethical Principles for Medical Research Regarding Human Subjects*. Available online at: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/

Conflict of Interest Statement: KM and PM are founders and owners of Biosecure Ltd. Biosecure Ltd. does not, and has not, received US Federal research funding.

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

The reviewer GK declared a past collaboration with one of the authors, PM, to the handling editor.

frontiers in Bioengineering and Biotechnology

PERSPECTIVE
published: 25 February 2019
doi: 10.3389/fbioe.2019.00021

National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data

Kavita M. Berger[1]* *and Phyllis A. Schneck*[2]

[1] Gryphon Scientific, LLC, Takoma Park, MD, United States, [2] Promontory Financial Group, an IBM Company, Washington, DC, United States

Biology and biotechnology have changed dramatically during the past 20 years, in part because of increases in computational capabilities and use of engineering principles to study biology. The advances in supercomputing, data storage capacity, and cloud platforms enable scientists throughout the world to generate, analyze, share, and store vast amounts of data, some of which are biological and much of which may be used to understand the human condition, agricultural systems, evolution, and environmental ecosystems. These advances and applications have enabled: (1) the emergence of data science, which involves the development of new algorithms to analyze and visualize data; and (2) the use of engineering approaches to manipulate or create new biological organisms that have specific functions, such as production of industrial chemical precursors and development of environmental bio-based sensors. Several biological sciences fields harness the capabilities of computer, data, and engineering sciences, including synthetic biology, precision medicine, precision agriculture, and systems biology. These advances and applications are not limited to one country. This capability has economic and physical consequences, but is vulnerable to unauthorized intervention. Healthcare and genomic information of patients, information about pharmaceutical and biotechnology products in development, and results of scientific research have been stolen by state and non-state actors through infiltration of databases and computer systems containing this information. Countries have developed their own policies for governing data generation, access, and sharing with foreign entities, resulting in asymmetry of data sharing. This paper describes security implications of asymmetric access to and use of biological data.

Keywords: biotechnology, cybersecurity, information security, data vulnerability, biological data, biosecurity, data access, data protection

OPEN ACCESS

Edited by:
Randall Steven Murch, Virginia Tech, United States

Reviewed by:
Segaran P. Pillai, United States Department of Homeland Security, United States
Jacqueline Fletcher, Oklahoma State University, United States

***Correspondence:**
Kavita M. Berger
kberger@gryphonscientific.com

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

Received: *29 November 2018*
Accepted: *29 January 2019*
Published: *25 February 2019*

Citation:
Berger KM and Schneck PA (2019) National and Transnational Security Implications of Asymmetric Access to and Use of Biological Data. Front. Bioeng. Biotechnol. 7:21. doi: 10.3389/fbioe.2019.00021

INTRODUCTION

Advances in computer science, engineering, and data science have changed research, development, and application of biology and biotechnology in the United States and internationally. Examples of changes include: (a) increased reliance on internet connectivity for research and laboratory operations (Accenture, 2015; Bajema et al., 2018; Olena, 2018); (b) increased use of automation in life-science laboratories (Chapman, 2003); (c) application of the "design-build-test" paradigm to create new biological organisms (Agapakis, 2014; Carbonell et al., 2018); (d) increased generation, analyses, and computational modeling of information about biological systems, cells,

and molecules (Thurow et al., 2004; Walpole et al., 2013); (e) treatment of organisms and DNA as materials rather than phenomena to study (Service, 2017; Anderson et al., 2018; Patel, 2018); and (f) new funders such as venture capital, crowdfunding platforms, and foreign companies and governments (Von Krogh et al., 2012; Cha, 2015; Mervis, 2017). These changes have transformed the scientific, agricultural, and health communities' ability to understand and manipulate the world around them. In addition, the changes have enabled an influx of new practitioners and problem-solvers into biology, providing opportunities for education and research all over the world.

Biotechnology harnesses the capabilities of computer, data, and engineering sciences to establish and advance new fields such as synthetic biology, precision medicine, precision agriculture, and systems biology. Cloud-based platforms and open source, easy-to-use software enable scientists from anywhere in the world to use advanced data analytics in their studies. The software and hardware emerging from these fields improve our collective understanding of molecular and systems-level genetics, new drug therapies for longer and better quality of life, and design of novel and/or unnatural organisms. Critical to these pursuits is the sharing of research results and underlying data, without which societal decision-making about human, animal, plant, and environmental health cannot be realized fully. However, during the past two decades, concerns about data sharing have been raised, resulting in the issuance of international, regional, and national-level policies governing access to different types of data, including biological data. In addition, the platforms through which data are stored, transported, and analyzed may be vulnerable to unauthorized acquisition of information by malicious actors, which could lead to significant economic and physical harms to the health, safety, and security of a population. Although not considered "dual use life sciences research of concern" U. S. Government, 2012, 2014), the potential for both benefit and risk to humanity meets the spirit of the dual use concept (National Research Council, 2004). Given the significant benefits afforded by data sharing and analysis, this paper highlights current data protection policies, potential risks of data exploitation by malicious actors, and potential strategies to mitigate those risks and promote rapid recovery in biotechnology fields that are breached.

The interconnectedness between the digital and biological worlds can be exploited by state actors, malicious nonstate actors, and hackers through a variety of means, resulting in harmful consequences from potential theft of information, promulgation of incorrect information, and/or disruption of activities (Lord and Forbes Technology Council, 2017; Souza, 2018; Ward, 2018). For example, theft of proprietary information from a pharmaceutical or biotechnology company may reveal trade secrets and allow competitors to develop superior products and/or bring existing products to market more quickly (Friedman, 2013), stifling innovation in the global commercial market and allowing adversaries to create harmful, untested therapies. Another example is theft of hundreds of millions of electronic healthcare records, the uses of which are not clear (Bogle, 2018; Cohen, 2018; Healthare IT News Staff, 2018; Huang and Steger, 2018; Keown, 2018). Although unauthorized access to protected data may be aided by technical vulnerabilities in networked computer systems, poor security practices, insider threats in academia, industry, and health facilities, and legal business dealings also can enable adversary access to such data (Lynch, 2017; Rappeport, 2018; South China Morning Post, 2018; Zhu, 2018). For examples, more than half of all data breaches at healthcare facilities are caused by healthcare personnel errors, a quarter of which resulted in unauthorized access to or disclosure of patient records through sharing of unencrypted information, sending information to the wrong patients, and accessing the data without authorization (Bai et al., 2017; Michigan State University, 2018). In addition, the Federal Bureau of Investigation (FBI) has raised national security concerns about foreign access to genomic data of U.S. citizens through legitimate scientific collaboration, funding of scientific research, investment in genomic sequencing companies [e.g., China-based WuXi Healthcare Ventures investment in the U.S.-based 23andMe (Biospace, 2015; Mui, 2016)], and purchase of companies (e.g., Complete Genomics) (Baker, 2012; GenomeWeb, 2012). As vulnerabilities are created through scientific advances, such as the use of machine learning algorithms to trick fingerprint authentication systems, new risks are identified (Bontrager et al., 2018; Nyu Tandon School of Engineering, 2018). Some of these concerns have resulted in the passage of the 2018 Foreign Investment Risk Review Modernization Act, which has initiated reform of the U.S. Government process for evaluating foreign investment in U.S. entities and export control of emerging technologies (Rappeport, 2018; U.S. Congress, 2018). Yet, these policy activities largely are reactive, rather than proactive.

CURRENT APPROACHES FOR PROTECTING DATA

Preventing accidental and deliberate risks typically involves the use of cyber and information security systems that include technological and behavioral solutions. Protection of laboratory control systems, computer networks, and databases often involves the use of technological solutions. However, some risks are addressed better through training of personnel to recognize and report phishing attempts, ensure sensitive information is encrypted, and prevent unauthorized individuals from gaining access to sensitive data, databases, and computer networks. To enhance security, policies for promulgating these practices for specific materials and information have been issued. For example, the U.S. Biological Select Agents and Toxins Regulations include guidance for network security to prevent failure of laboratories, equipment, and access controls to facilities and data (Federal Select Agent Program, 2017). In addition, the U.S. has policies for protecting individual privacy, several of which were described in a 2014 report sponsored by the White House (Podesta et al., 2014). However, error, carelessness, or negligence by personnel can counteract the benefits afforded by security measures and may lead to devastating consequences if biological data and materials are involved.

Although policies for protecting biological data from cyberattack are limited, policies that govern data access and sharing are prevalent. These top-down, data access policies intend to protect individual rights and/or prevent sharing or distribution of data, including biological data. Examples of recent policies include: (a) the 2018 update of the European Union General Data Protection Regulation (European Commission, 2018), which strengthened the European Union's rules for protecting personal data of individuals, in part by giving its citizens "more control over their personal data;" (b) the 2018 Chinese Personal Information Security Specification, which is one system under the Chinese Cybersecurity law, involves the "collection, storage, use, sharing, transfer, and disclosure of personal information," and enables companies operating in China to access data to "not hamper the development of fields like AI" (Sacks, 2018); (c) the 2018 General Data Protection Law in Brazil, which provides a framework for the use of personal data in Brazil (Soares, 2018); and (d) the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), which promotes the protection of privacy and security of patient health information in the United States (Department of Health and Human Services, 2017). At the same time, the U.S. has issued policies governing data generation, access, and sharing to promote information-sharing and transparency of government-sponsored research (Noorden, 2013). Internationally, the Nagoya Protocol of the Convention on Biodiversity[1] promotes governance on access to and fair, equitable sharing of the benefits from the use of non-human biological data. However, questions exist about whether the Nagoya Protocol focuses more on biological samples that provide genetic information or the genetic information itself, which ultimately affects national-level efforts for codifying the international agreement (Dos et al., 2018). Despite these activities, protection of some data, such as personal health data, may not extend beyond a country's borders and may apply only to data collected by certain entities. Furthermore, data protection polices do not extend to information that already has been stolen. Taken together, these national, regional, and international level policies for data protection may not prevent the inappropriate or unauthorized acquisition of data to different actors, the consequences of which are unclear for biotechnology data.

VULNERABILITY OF BIOTECHNOLOGY DATA

The primary challenges in identifying, assessing, and mitigating security vulnerabilities of biotechnology data are understanding: (a) how the data may be exploited by adversaries and what consequences result from this exploitation; and (2) what potential negative effects may arise from digitalization of biotechnology and advanced computation of biological data (Bajema et al., 2018). The term "biotechnology" refers to the exploitation of biological processes for industrial and scientific purposes, and includes genetic manipulation of microbes, plants, animals, human cells, nucleic acids (the building blocks of genomes), and proteins (the functional units in cells). This definition is expanded further to include generation, incorporation, and use of digital forms of biological data. These biological data may be available online through databases, such as the U.S. National Center for Biotechnology Information's GenBank[2], or generated in a laboratory and stored, shared, and/or analyzed locally or remotely (via online and/or cloud-based software). By attempting to answer the questions posed above, specific risks associated with the legal and illegal acquisition of biological data may be identified and mitigated.

Although extraordinary advances in computing power are enabling unprecedented scientific discoveries, its application to biology and healthcare is increasing without effective protection from the risks of adversary acquisition or accidental misuse of information. Scientific data that is generated in basic and applied research laboratories in academia, non-profit research organizations, service providers, and some industry research facilities may be considered fundamental research destined for publication and public benefit. These data are not necessarily sensitive, but they do represent the results of significant investment by governments, industry, investors, and philanthropic organizations. Therefore, theft or large-scale acquisition of these data may have adverse economic consequences to the organization, field, or nation, especially if acquisition was directed by adversarial nation-states to gain competitive advantage in a given sector (Blair and Huntsman, 2013). As previously described, databases that store sensitive and/or non-sensitive biological data have been infiltrated by external actors and accessed by unauthorized individuals. Although measures to protect data have been implemented in several institutions, cyber and information security policies, practices, and compliance vary across biotechnology sectors, location, and organization type (e.g., academia, industry). Although implementation of cyber, information, and data security in biological facilities can help to minimize the potential for deliberate or accidental release of protected biological data, these measures are insufficient on their own (Press, 2018).

Furthermore, the increasing size and volume of the datasets, and the complexity of analytic technologies has led many scientists to rely on cloud-based platforms to store, transfer, and analyze data. These platforms and technologies, including online analysis software and applications, often do not prevent unauthorized access to data or ensure software fidelity. Although mitigating specific vulnerabilities may be possible on an individual platform or technology level, implementing protections across the various data generation, analysis, transfer, and storage platforms currently in use in academia, industry, government laboratories, and healthcare facilities is challenging. Countering these risks requires the identification of consequences that are of particular concern to public safety

[1]Convention on Biodiversity. About the Nagoya Protocol. Available online at: https://www.cbd.int/abs/about/ (Accessed November 23, 2018).

[2]National Center for Biotechnology Information. GenBank. Available online at: https://www.ncbi.nlm.nih.gov/genbank/ (Accessed November 23, 2018).

and national security, evaluation of vulnerabilities that may enable the realization of these consequences, and identification of measures to address these vulnerabilities.

POSSIBLE PREVENTION AND MITIGATION APPROACHES

Modern cyber and information security reflects the risks experienced as the internet has grown and diversified, and as the capabilities for and speed of storing, processing, and transporting information have increased exponentially (Denning and Lewis, 2017). The internet was built without a priority on the protection of data whether "at rest" (i.e., stored data) or "in motion" (i.e., data in transit) (Dauch et al., 2009; Inap, 2013). Current strategies for addressing cyber risks focus on remediation through regulation, organizational support, and actions taken by data owners and consumers in the form of encryption technologies, access control measures, awareness-raising campaigns, risk assessment, blocking, limiting publication of sensitive information, and other similar practices. The challenge is understanding how these measures are to be applied to biotechnology data, how to balance the cost of implementation with the consequences if left unprotected, and what vulnerabilities cannot be mitigated using commercial products.

Often the entities that assess their cyber vulnerabilities and invest in cyber and information security measures are compelled to do so because of regulation and fiscal responsibility (McDonald, 2017). However, unlike financial information, biotechnology data is regulated in some countries, but not others. For example, China issued a recent policy requiring a domestic collaborator and Ministry-level approval for research involving genomic data of Chinese citizens and/or biological samples obtained in China to prevent exploitation of these data and samples (Tuzman, 2018). This and similar policies raise questions about their intended and unintended effects to nations, to the scientific community, and to international security mainly because the policies that may benefit one country could harm another. These harms may reveal new types of risks associated with the acquisition and use of data to manipulate biological systems. These risks may be perpetrated by different actors; affect sector and country economies, commercial biotechnology, and pharmaceutical markets domestically and internationally; and alter global strategic power dynamics.

The risks associated with biotechnology data do not conform to traditional biosecurity concerns, which focus primarily on risks to human health or the food and agriculture economy. These risks involve multiple domains, sectors, and nations resulting in outcomes such as shifting of balance of power of nations at the international level, which could have downstream effects on areas that overlap with biosecurity interests (e.g., biosafety and biosecurity, biothreat reduction, and global health security). Strategies for bridging the biological, cyber, information, and data security include: (a) collaboration between the biological and cybersecurity communities; (b) end-to-end risk assessments; (c) data-specific risk and vulnerability assessments; and (d) application of the NIST Cybersecurity Framework for protecting biological data.

Formal collaboration between the biotechnology and biological, information, data, and cyber security communities would enhance efforts toward identification of risks and vulnerabilities associated with data management, provenance, and integrity, and risk mitigation strategies. Technologies are readily available to protect data, but their use must be harmonized worldwide, because protecting data in one database is ineffective if another database remains vulnerable to external threats. Furthermore, organizations may evade regulatory requirements and industry standards in protecting data because of perceived lack of cost savings for implementing cybersecurity measures or lack of awareness of the risks, which could lead to investor, intruder, or adversary access to sensitive information that may be stored in databases or transferred between computers. These vulnerabilities may be exacerbated by limitations of national laws to other sovereign states, and differences in interpretation of the types of data included in the scope of existing laws. **Given these potential vulnerabilities, the cybersecurity and biotechnology communities must engage to create best practices and processes to protect data and mitigate risk while reaping the benefits of computing technology applications to biotechnology.**

End-to-end assessments of the data storage, processing, and transport pipeline can identify outstanding vulnerabilities and technical gaps that may be addressed with currently available cyber, information, and data security solutions. This process would enable identification of gaps for which these measures are insufficient and of institutions that are responsible for implementing controls. Without this type of assessment, vulnerabilities may exist along the pipeline without its users' knowledge. A lack of rigorous analysis makes biological data vulnerable to acquisition or alteration by witting adversaries, potentially resulting in theft of intellectual property for commercial gain, foreign government acquisition of genomic data from large portions of a population for undefined purpose or compromise of software and data integrity. At least one country promotes acquisition of data though legitimate commercial practices (e.g., providing sequencing services to customers; partnering with academia, independent research institutions, and universities; and foreign investment), talent promotion programs (Capaccio, 2018; Nature Jobs, 2018), and theft of data (Riley and Walcott, 2015; Dilanian, 2018; Kaiser and Malakoff, 2018; Wilber, 2018). The FBI has expressed concerns about the theft of U.S. genomics and health information through cyberattacks and foreign investment in the U.S. biotechnology industry (You, 2017). The FBI argues that acquisition of this information can give adversaries an unfair advantage in the international pharmaceutical or biotechnology marketplace. Others have expressed concern about questionable use of genetic information that countries obtain from their own citizens or from other countries' citizens (Human Rights Watch, 2017; Lynch, 2017; Pauwels and Vidyarthi, 2017). **These risks could be addressed by conducting an end-to-end risk assessment of the software**

and equipment involved in the data pipeline within individual organizations, between organizations, and across countries.

Defining the consequences of greatest concern to national security is an initial step toward assessing the risks and vulnerabilities of the information itself and data-specific risk mitigation strategies. Evaluating these risks enables the identification of content-specific approaches for detecting and countering exploitation of vulnerabilities by insider and external actors. Without these assessments, only generic cyber and information security measures will be implemented. However, these measures are insufficient to counter adversaries who are intent on acquiring data through a variety of technical, social engineering, or other means. Given this reality, rapid detection and resilience (i.e., rapid recovery after a breach) are critical for reaping the benefits and minimizing the vulnerabilities of advanced electronic computation and mass connectivity. In 2014, the White House explored technology needs for protecting the security and privacy of exposed data, including healthcare data (Executive Office of the President, 2014; President's Council of Advisors on Science Technology, 2014). But, these studies did not define consequences of concern related to the unauthorized acquisition of vast amounts of biological data, effectively limiting the identification of data-specific or process-specific prevention measures. **Therefore, risk assessments of specific types of data are equally as important to conduct as analyses of vulnerabilities of laboratory control systems, data management platforms, and computer networks.**

Application of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to all systems of storage, processing and transport of biological data would help explore where, how, and by whom data is processed with the goal of protecting valuable scientific and health information (National Institute of Standards Technology, 2018). The NIST framework involves a collaboration of private sector and government cybersecurity experts that seek to apply the five principles of data protection (i.e., identify, protect, detect, respond, and recover) to systems, including those on which biological data are generated, processed and transported. The framework could augment existing or newly-implemented efforts of vulnerability detection and mitigation, thus decreasing unauthorized exposure of sensitive data. The NIST framework is a widely accepted paradigm for cyber risk management and best practices (Department of Homeland Security, 2018; Lohrmann, 2018; Roncevich, 2018). In the U.S., this framework has been used in regulatory dialogues to demonstrate rigor toward cybersecurity in sectors for which such requirements are not well-documented in law. **Application of the NIST framework to biotechnology can enhance data protection and a focus on rapid detection of nefarious activity and resiliency after an attack.**

These suggestions describe various approaches toward protecting biological data from unauthorized acquisition and use, enhancing efforts to preserve data integrity and provenance, and enabling future benefit of biotechnological advances.

AUTHOR CONTRIBUTIONS

KB and PS contributed equally to this manuscript. The concepts, conclusions, and recommendations were generated jointly by the authors and built on their respective expertise in the biological sciences and biosecurity, and computer science and cybersecurity.

REFERENCES

Accenture (ed). (2015). *The Future of Applications in Life Sciences: New application Strategies to Unlock the Digital Opportunity*. A.L. Sciences.

Agapakis, C. M. (2014). Designing synthetic biology. *ACS Synth. Biol.* 3, 121–128. doi: 10.1021/sb4001068

Anderson, L. A., Islam, M. A., and Prather, K. L. J. (2018). Synthetic biology strategies for improving microbial synthesis of "green" biopolymers. *J. Biol. Chem.* 293, 5053–5061. doi: 10.1074/jbc.TM117.000368

Bai, G., Jiang, J. X., and Flasher, R. (2017). Hospital risk of data breaches. *JAMA Intern. Med.* 177, 878–880. doi: 10.1001/jamainternmed.2017.0336

Bajema, N. E., Dieuliis, D., Lutes, C., and Lim, Y.-B. (2018). "The digitalization of biology: understanding the new risks and implecations for governance," in *Emergence and Convergence*, ed National Defense University (Washington, DC: National Defense University), 2–3, 7–12.

Baker, M. (2012). China buys US sequencing firm. *Nature* 489, 485–486. doi: 10.1038/489485a

Biospace (2015). *WuXi Healthcare Invests in US Genomics Testmaker 23andMe*. BioSpace. Available online at: https://www.biospace.com/article/releases/-b-wuxi-healthcare-b-invests-in-us-genomics-testmaker-23andme-/

Blair, D. C., and Huntsman, J. M. (2013). *The Report of the Commission on the Theft of American Intellectual Property*. ed T. I. Commission (The National Bureau of Asian Research).

Bogle, A. (2018). *Healthcare Data a Growing Target for Hackers, Cyberseucrity Experts Warn*. ABC News. Available online at: https://www.abc.net.au/news/science/2018-04-18/healthcare-target-for-hackers-experts-warn/9663304 (Accessed November 23, 2018).

Bontrager, P., Roy, A., Togelius, J., Memon, N., and Ross, A. (2018). DeepMasterPrints: generating masterprints for dictionary attacks via latent variable evolution. *arXiv*.

Capaccio, A. (2018). *U.S. Faces 'Unprecidented Threat' From China on Tech Takeover*. Bloomberg. Available online at: https://www.bloomberg.com/news/articles/2018-06-22/china-s-thousand-talents-called-key-in-seizing-u-s-expertise (Accessed November 23, 2018).

Carbonell, P., Jervis, A. J., Robinson, C. J., Yan, C., Dunstan, M., Swainston, N., et al. (2018). An automated design-build-test-learn pipeline for enhanced microbial production of fine chemicals. *Commun. Biol.* 1:66. doi: 10.1038/s42003-018-0076-9

Cha, A. E. (2015). Crowdfunding propels scientific research. *The Washington Post*.

Chapman, T. (2003). Lab automation and robotics: automation on the move. *Nature* 421, 665–666. doi: 10.1038/421665a

Cohen, J. (2018). *Massive Cyberhack by Iran Allegedly Stole Research from 320 Universities, Governments, and Companies*. Science. Available online at: https://www.sciencemag.org/news/2018/03/massive-cyber-hack-iran-allegedly-stole-research-320-universities-governments-and

Dauch, K., Hovak, A., and Nestler, R. (2009). "Information assurance using a defense in-depth strategy," in *Conference For Homeland Security, 2009 CATCH'09, Cybersecurity Applications and Technology* (Washington, DC), 267–272.

Denning, P. J., and Lewis, T. G. (2017). Exponential laws of computing growth. *Commun. ACM.* 60, 54–65. doi: 10.1145/2976758

Department of Health and Human Services (2017). *Summary of the HIPAA Security Rule*. Washington, DC. Available online at: https://www.hhs.gov/

hipaa/for-professionals/security/laws-regulations/index.html (Accessed November 23, 2018).

Department of Homeland Security (2018). *Using the Cybersecurity Framework*. Available online at: https://www.dhs.gov/using-cybersecurity-framework (Accessed January 24, 2019).

Dilanian, K. (2018). *China's Hackers Are Stealing Secrets From U.S. Firms Again, Experts Say*. NBC News. Available online at: https://www.nbcnews.com/news/china/china-s-hackers-are-stealing-secrets-u-s-firms-again-n917836 (Accessed January 27, 2019).

Dos, S. R. C., Koopmans, M. P., and Haringhuizen, G. B. (2018). Threats to timely sharing of pathogen sequence data. *Science* 362, 404–406. doi: 10.1126/science.aau5229

European Commission (2018). *2018 Reform of EU Data Protection Rules*. European Commission.

Executive Office of the President (2014). *Big Data: Seizing Opportunities, Preserving Values*. Washington, DC: White House.

Federal Select Agent Program (2017). *Information Systems Security Controls Guidance*. Atlanta, GA.

Friedman, A. A. (2013). *Cyber Theft of Competitive Data: Asking the Right Questions*. Brookings Institution.

GenomeWeb (2012). *Complete Genomics, BGI Agree to $117.6M Merger*. GenomeWeb. Available online at: https://www.genomeweb.com/sequencing/complete-genomics-bgi-agree-1176m-merger#.XEqIOFxKiUl (Accessed January 24, 2019).

Healthare IT News Staff (2018). *The Biggest Healthcare Data Breaches of 2018 (So Far)*. Healthcare IT News. Available online at: https://www.healthcareitnews.com/projects/biggest-healthcare-data-breaches-2018-so-far (Accessed November 23, 2018).

Huang, E., and Steger, I. (2018). *China is Secretly Enrolling Military Scientists in Western Universities*. Defense One. Available online at: https://www.defenseone.com/threats/2018/10/china-secretly-enrolling-military-scientists-western-universities/152383/?oref=d-mostread (Accessed November 23, 2018).

Human Rights Watch (2017). *China: Minority Region Collects Data from Millions*. New York, NY: Human Rights Watch.

Inap (2013). *Data in Motion vs. Data at Rest*. Available online at: https://www.inap.com/blog/data-in-motion-vs-data-at-rest/ (Accessed January 24, 2019).

Kaiser, J., and Malakoff, D. (2018). NIH investigating whether U.S. scientists are sharing ideas with foreign governments. *Science*. doi: 10.1126/science.aav2343

Keown, A. (2018). *Second Scientist Pleads Guilty to Steeling GlaxoSmithKline Trade Secrets*. BioSpace. Available online at: https://www.biospace.com/article/-jc1n-second-scientist-pleads-guilty-to-stealing-glaxosmithkline-trade-secrets/ (Accessed November 23, 2018).

Lohrmann, D. (2018). *Why You Need the Cybersecurity Framework*. Government Technology.

Lord and Forbes Technology Council (2017). *The Real Threat Of Identity Theft Is In Your Medical Records, Not Credit Cards*. Forbes.

Lynch, D. J. (2017). *Biotechnology: the US-China Dispute over Genentic Data*. Financial Times. Available online at: https://www.ft.com/content/245a7c60-6880-11e7-9a66-93fb352ba1fe (Accessed November 23, 2018).

McDonald, K. (2017). *Private Sector's National Cybersecurity Strategy Contributions Lacking*. TechTarget. Available online at: https://searchcompliance.techtarget.com/opinion/Private-sectors-national-cybersecurity-strategy-contributions-lacking (Accessed January 24, 2019).

Mervis, J. (2017). Data check: U.S. government share of basic research funding falls below 50%. *Science*. doi: 10.1126/science.aal0890

Michigan State University (2018). *Healthcare Providers - Not Hackers - Leak More of Your Data*. EurekAlert!. Available online at: https://eurekalert.org/pub_releases/2018-11/msu-hp-111618.php (Accessed November 23, 2018).

Mui, Y. Q. (2016). *China's $9 Billion Effort to Beat the U.S. in Genetic Testing*. The Washington Post. Available online at: https://www.washingtonpost.com/news/wonk/wp/2016/12/30/chinas-9-billion-effort-to-beat-the-u-s-in-genetic-testing/?noredirect=on&utm_term=.3a83001d622d

National Institute of Standards and Technology (2018). *NIST Cybersecurity Framework*. ed D.O. Commerce. Washington, DC.

National Research Council (2004). *Biotechnology Research in an Age of Terrorism*. Washington, DC: National Academies Press.

Nature Jobs (2018). *China's Plan to Recruit Talented Researchers*. Career Guide. Available online at: https://www.nature.com/articles/d41586-018-\penalty-\@M00538-z

Noorden, R. V. (2013). *White House Announces New US Open-Access Policy*. Nature. Available online at: http://blogs.nature.com/news/2013/02/us-white-house-announces-open-access-policy.html (Accessed November 23, 2018).

Nyu Tandon School of Engineering (2018). *Machine Learning Masters the Fingerprint to Fool Biometric Systems*. PR Newswire. Available online at: https://www.prnewswire.com/news-releases/machine-learning-masters-the-fingerprint-to-fool-biometric-systems-300753375.html

Olena, A. (2018). *Bringing the Internet of Things into the Lab*. The Scientist.

Patel, P. (2018). *DNA Data Storage Gets Random Access*. IEEE Spectrum.

Pauwels, E., and Vidyarthi, A. (2017). "Who will own the secrets in our genes? A U.S.-China race in artificial intelligence and genomics," in *Wilson Briefs*, ed W. W. Center (Washington, DC: Woodrow Wilson Center for International Scholars), 5–9.

Podesta, J., Pritzker, P., Moniz, E. J., Holdren, J., and Zientz, J. (2014). *Big Data: Seizing Opportunities, Preserving Values*. ed E.O.O.T. President (Washington, DC).

President's Council of Advisors on Science and Technology (2014). *Big Data and Privacy: A Technological Perspective*. ed E.O.O.T.U.S. President (Washington, DC: White House).

Press, G. (2018). *60 Cybersecurity Predictions for 2019*. Forbes.

Rappeport, A. (2018). *In New Slap at China, U.S. Expands Power to Block Foreign Investments*. The New York Times. Available online at: https://www.nytimes.com/2018/10/10/business/us-china-investment-cfius.html (Accessed November 23, 2018).

Riley, M., and Walcott, J. (2015). *China's Hack of U.S. Data Tied to Health-Care Record Thefts*. Bloomberg UNE.

Roncevich, T. (2018). *Healthcare IT Security Best Practices: Adopting NIST's Cybersecurity Framework. Cyberguard Compliance*. Available online at: https://info.cgcompliance.com/blog/healthcare-it-security-best-practices-adopting-nists-cybersecurity-framework (Accessed Jan 24, 2019).

Sacks, S. (2018). *China's Emerging Data Privacy System and GDPR*. Washington, DC: Center for Strategic and International Studies.

Service, R. F. (2017). DNA could store all of the world's data in one room. *Science*. doi: 10.1126/science.aal0852

Soares, E. (2018). *Brazil: Personal Data Protection Law Enacted. Global Legal Monitor*. Available online at: https://www.loc.gov/law/foreign-news/article/brazil-personal-data-protection-law-enacted/ (Accessed November 23, 2018).

South China Morning Post (2018). *Chinese Funds Pour US$1.4b into US Biotechnology Firms in the First Three Months of the Year*. South China Morning Post. Available online at: https://www.scmp.com/business/global-economy/article/2142351/chinese-funds-pour-us14b-us-biotechnology-firms-first-three (Accessed November 23, 2018).

Souza, C. (2018). *Lessons for Pharma from the Merck Cyber Attack*. PharmExec.com. Available online at: http://www.pharmexec.com/lessons-pharma-merck-cyber-attack (Accessed January 21, 2019).

Thurow, K., Gode, B., Dingerdissen, U., and Stoll, N. (2004). Laboratory information management systems for life science applications. *Org. Proc. Res. Dev.* 8, 970–982. doi: 10.1021/op040017s

Tuzman, K. T. (2018). *Border Security for China's Genomes*. Biocentury Innovations. Available online at: https://www.biocentury.com/bc-innovations/strategy/2018-10-11/balancing-protection-and-translation-china%E2%80%99s-genomic-data-troves

U.S. Congress (2018). *Foreign Investment Risk Review Modernization Act*.

U. S. Government (2012). *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern*. Washington, DC.

U. S. Government (2014). *United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern*, Washington, DC.

Von Krogh, G., Battistini, B., Pachidou, F., and Baschera, P. (2012). The changing face of corporate venturing in biotechnology. *Bioentrepreneur* 30, 911–915. doi: 10.1038/bioe.2012.9

Walpole, J., Papin, J. A., and Peirce, S. M. (2013). Multiscale computational models of complex biological systems. *Annu. Rev. Biomed. Eng.* 15, 137–154. doi: 10.1146/annurev-bioeng-071811-150104

Ward, A. (2018). *ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa*. RAND. Available online at: https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html (Accessed January 21, 2019).

Wilber, D. Q. (2018). Chinese hackers charged with stealing data from Navy, JPL and U.S. companies. *LA Times*.

You, E. H. (2017). *Safeguarding the Bioeconomy: U.S. Opportunities and Challenges, Testimony for the U.S.-China Economic and Security Review Commission*. Washington, DC: F.B.O. Investigation.

Zhu, J. (2018). *As China Builds Biotech Sector, Cash Floods U.S. Startups*. Reuters. Available online at: https://www.reuters.com/article/us-biotech-china-investment/as-china-builds-biotech-sector-cash-floods-u-s-startups-idUSKCN1M400G (Accessed November 23, 2018).

Disclaimer: The views and conclusions contained herein are those of the authors and should not be interpreted as representing the views and conclusions or official policies and endorsements, either expressed or implied of Griffin Scientific, Promontory Financial Group or the U.S. Government.

Conflict of Interest Statement: KB was employed by Gryphon Scientific. PS was employed by Promontory Financial Group, which is an IBM Company.

The authors declare that the paper was written in the absence of any commercial or financial relationships that would constitute a conflict of interest.

frontiers in Bioengineering and Biotechnology

PERSPECTIVE
published: 22 March 2019
doi: 10.3389/fbioe.2019.00051

The National Security Implications of Cyberbiosecurity

*Asha M. George**

Blue Ribbon Study Panel on Biodefense, Washington, DC, United States

The cyber- and biological sciences are converging rapidly, creating benefits, new and advantageous applications, and increasing risks to all nations. The parts of the public and private sectors that should be responsible for cyberbiosecurity are not yet sufficiently organized or supported financially. This article addresses the need to ensure that national security policy: (1) assesses cyberbiological risk and incorporates deterrent and enforcement measures; (2) sets forth clear consequences for those individuals and countries that conduct cyberbiological attacks or otherwise compromise cyberbiosecurity, without imperiling the legitimate sharing of scientific data and information; (3) establishes voluntary cyberbiosecurity standards in partnership with the private sector; (4) identifies cyberbiosecurity threats, vulnerabilities, consequences, and solutions; and (5) results from the combined efforts of all branches of government and the private sector.

Keywords: cyberbio, cyberbiosecurity, cybersecurity, biosecurity, convergence

OPEN ACCESS

Edited by:
Randall Steven Murch, Virginia Tech, United States

Reviewed by:
Gerald Epstein, National Defense University, United States
Calvin Chue, U.S. Army Edgewood Chemical Biological Center (ECBC), United States

***Correspondence:**
Asha M. George
asha.george@biodefensestudy.org

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

Received: *26 November 2018*
Accepted: *01 March 2019*
Published: *22 March 2019*

Citation:
George AM (2019) The National Security Implications of Cyberbiosecurity. Front. Bioeng. Biotechnol. 7:51. doi: 10.3389/fbioe.2019.00051

INTRODUCTION

Many fields of science depend on and are affected by the cyber revolution. The far older field of biology is no exception. In fact, the two fields of biology (the science of life and living organisms, including their physical, chemical, molecular, physiological, and developmental characteristics) and cyberology (the science, study, and theory of cyberspace and cybernetics, including communications over computer networks, Internet-connected systems and data centers, computerized systems, communications and automatic control systems in both machines, and living things) are not only interrelated, each can offer perspectives on the other, enabling greater understanding while simultaneously multiplying the possibilities for new, combined threats, previously unanticipated vulnerabilities, and unintended consequences. Murch et al. (2018) defined cyberbiosecurity as "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, 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." Adequate cyberbiosecurity can only be achieved by taking both cyber- and biological perspectives into consideration simultaneously.

CYBERBIO CONVERGENCE

Lateral thinking intentionally connects disparate subjects to generate new ideas, products, and solutions (de Bono, 1970). Additionally, different scientific areas also converge as we gain greater understanding of their most basic, often elemental characteristics, and comprehend their similarities and sometimes, equivalence (Sharp et al., 2011). Convergence also occurs through the

intentional combination of two different fields, using aspects of both to produce something new (Roco and Bainbridge, 2002).

The adjective cyberbio results from all three of these types of convergence. We laterally apply our understanding of biology to robotics, nanotechnology, data, cyberspace, cybernetics, and other cyber-related areas, just as we take our understanding of cyberology and look for the same in biology and biological systems. Organic material developed artificially and used in cyber-enabled technologies and products sometimes behaves in the same way as naturally occurring organic material (Irving, 2017). As we combine the cyber- and biological fields, we create new cyberbio threats, vulnerabilities, and consequences.

National security communities throughout the world cannot afford to ignore cyberbio convergence and the increased requirements for cyberbiosecurity associated with it. As with many scientific advancements, the challenge lies in preventing intended and unintended negative impacts on every nation (Sherden, 2011). Additionally, given the speed at which both cyber- and biological activity can occur independently, the separation between and among nations is already very small. Combined cyberbio activity could move even faster, rendering geographic separation non-existent.

Many critical infrastructure sectors can be affected, and as a result, they must play a role in assuring cyberbiosecurity. The Chemical (particularly due to the convergence of biology and chemistry), Critical Manufacturing, Defense Industrial Base, Emergency Services, Energy, Food and Agriculture, Healthcare and Public Health, and Information Technology Sectors are most affected. While some may be aware of the cyberbiological risk to their sectors, they have not yet determined how best to defend against individual cyber- and biological, let alone combined cyberbiological, risks.

Cyberbio deterrence and enforcement pose challenges for national security policymakers (Blue Ribbon Study Panel on Biodefense., 2015). It is unclear what deterrence measures can be developed or enforced in this regard, especially when deterrence and enforcement are lacking for cyber- and biological activities, individually. With regard to cybersecurity, increased support for overt counter-cyber activities and dedicated cybersecurity agencies (e.g., the governmental mitosis that first resulted in the National Security Agency and U.S. Cyber Command, and then other federal organizations, such as the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, in the United States) may appear to be so large or prolific as to serve as deterrents, but it unclear how effective they will be (Nakashima, 2018). The Biological and Toxin Weapons Convention (Findlay, 2006), programs to control biological select agents (US Government Accountability Office, 2017), and laws and regulations prohibiting the use of biological material for crime, terrorism, and warfare (Hodge, 2012), create some barriers to misuse and establish some agreed upon national and international norms, but serve as imperfect deterrents in the biological arena. Deterrents and laws preventing malevolent cyberbio activity have not been legislated in many countries. Extant legislation addressing cyber- and biological risks lags behind technological advances in these fields and cannot be depended upon to address combined cyberbiological threats, vulnerabilities, and consequences.

CONSEQUENCES WITHOUT IMPERILING LEGITIMATE INFORMATION SHARING

The biological research community depends on digital systems to store and analyze data (Schatz, 2015). Of great concern are the huge amounts of data accessible via the Internet and various Cloud applications, with inadequate cybersecurity (Schneier, 2012). Intellectual property and proprietary information losses associated with digitized biological information could rise to the millions or billions, eventually resulting in economic decreases and reduced international competitiveness (Heus et al., 2017). Other national security concerns include loss of privacy, discrimination, data loss or theft, industrial and commercial sabotage, industrial hacking, exploitation of research to increase disease severity, targeting based on specific DNA patterns, and the production of dangerous and novel pathogens without physical samples (Bajema et al., 2018).

Many of the same countries that are investing large amounts in cutting-edge biological research and dual-use activities that could be used to produce biological weapons are also thought to be responsible for many of the cyber incidents with which the public and private sectors throughout the world struggle today. Advances in cyber- and biological science depend in large part on information systems and management, data storage, and the increased efficiency that computational analysis affords. Some countries may want data and information to feed their growing cyber- and biological weapons programs, increase disease and cyber-attack severity on enemy populations, target specific groups for attack, harm other economies, and boost their own economic competitiveness. Evidence of and information regarding cyberbio convergence and related products may well be the most valuable of all, allowing for the acceleration of nascent, ineffective, or slow-to-develop programs.

While we must encourage the legitimate sharing of scientific data and information, and comprehend that there are not yet reasonable or better alternatives to current cyber communications and data storage options, we must also recognize that all nations and their biological and cyberbiological research, development, science, and technology are at great risk. As a matter of national security, each country must require additional biosecurity and cybersecurity in this arena and set forth clear consequences for individuals and countries who intentionally breech whatever security measures they already utilize to obtain biological and cyberbiological data and information. We must also set forth clear consequences for individuals who do not take enough care to protect the data they generate. Increased cyberbiosecurity may make information sharing more difficult, but it will not make the legitimate sharing of data and information impossible.

ESTABLISHMENT OF VOLUNTARY CYBERBIOSECURITY STANDARDS

The public and private sectors agree with the need for increased cyberbiosecurity. No one is interested in losing their work to their competitors within or outside their organization, company, or country. No one is so naïve as to believe that the nobility of their

efforts somehow serves as a protective shield against those who want to further their own agenda.

Considering the vast number of cyber-, biological, and cyberbiological efforts currently underway, and the inability of the private sector to protect itself against all national security threats, national governments should work with their private sectors to establish voluntary standards for cyberbiosecurity. Even if governments possess enough knowledge of the breadth and specificity of private sector research and development, they generally have few mechanisms with which to force the private sector to protect against cyberbiological threats.

There are many models for the development and implementation of standards that both the public and private sectors agree to meet (National Research Council., 2015). Fewer models exist to successfully develop incentives for meeting, and agree upon penalties for not meeting, standards. The government must work with the private sector to develop cyberbiosecurity standards, incentives, and penalties within a specified, relatively short period (e.g., 1 year). The speed at which benevolent and malevolent activity is occurring defies the protracted consensus-driven processes in which many governments, such as that of the United States, engage (The White House., 1998).

IDENTIFICATION OF CYBERBIOLOGICAL RISK AND OTHER SOLUTIONS

While both cybersecurity and biosecurity efforts are underway (with more money and resources currently going to the former), there is an obvious gap when it comes to cyberbiosecurity. For example, even within the U.S. Department of Defense, which now possess two powerful cybersecurity organizational elements (i.e., National Security Agency, U.S. Cyber Command) as well as several organizations that conduct biological research and development using highly dangerous pathogens (e.g., U.S. Army Medical Research Institute of Infectious Diseases), efforts to ensure cyberbiosecurity are insufficient (Knapp, 2018). Governmental agencies throughout the world with responsibilities for agriculture, defense, energy, justice, labor, natural resources, and transportation address cyber- and biological threats separately. Departments of justice and other departments that investigate criminal and terrorism financing are also hobbled by weak or non-existent laws for cyberbiological and other new threats.

Some nations combine their military and intelligence activities. Others are fortunate enough to have enough resources to support both separately. In either case, military and intelligence communities throughout the world must acknowledge ongoing cyberbiological activities. These communities often lack the scientific and technological expertise needed to understand the state of science in the cyber- and biological fields, impact of their convergence, intended outcomes for investments in these areas, and how they could and do impact national security. Given the speed with which advances are occurring, intelligence communities throughout the world must assess cyberbiological capabilities, applications, and abilities to do harm. Military and other national security departments must utilize this intelligence to determine how best to protect national assets.

Each country needs a large-scale program to identify and assess cyberbiological risk. At a minimum, such a program should identify new cyberbio threats, vulnerabilities, and consequences (e.g., those associated with pathogen and biomanufacturing data systems, dual-use synthetic biology, biological intellectual property, bioeconomy). This program should result from a public-private partnership among all government agencies, and private sector companies, academic institutions, and other non-governmental organizations. Risk analysis should be rigorous, independent, critical, and comprehensive, utilizing the same or similar methodologies already developed for systems analysis.

As with all areas which are converging presently, expertise is usually very hard to come by. There are some, however, who have worked in or with both fields, who could serve as effective translators between the cyber- and biological communities. Lateral thinkers, who know how to expertly apply knowledge gained in one area to that of another to come up with new insights can also be effectively utilized. As with all relatively new threats, few experts exist now with operational expertise, but they can be developed through academic and operational training and education programs. Intelligence communities should seek to develop insiders involved in cyberbio activities. Public and private sector organizations that address futures must develop scenarios that are used to develop agricultural, diplomatic, healthcare, public health, and military requirements. Governmental and non-governmental scientists must work together to understand and address the problem, while simultaneously contributing to the cyberbio body of knowledge.

COMBINED GOVERNMENTAL EFFORTS

The legislative bodies and those government agencies responsible for implementing laws must work together to reduce national cyberbiological risk.

Legislative bodies must authorize national cyberbiosecurity programs that:

- Address cyberbiological risk and incorporate deterrent and enforcement measures;
- Set forth clear consequences for individuals or countries that undertake such actions without imperiling the legitimate sharing of scientific data and information;
- Allow for the establishment of voluntary standards in partnership with the private sector;
- Identify new cyberbiosecurity threats, vulnerabilities, and consequences; and
- Develop and implement solutions.

Knowing what a government must authorize is less difficult than determining legislative jurisdiction in the cyberbio arena. It is unrealistic to expect that different elements of legislative bodies that have historically addressed either cyber- or biological risk separately will suddenly or automatically work together to

develop and pass legislation that address cyberbiological risk. However, given the extremely large potential impact on each nation's bioeconomy, those legislative elements that address commerce, science, and security are best positioned to produce needed cyberbiological legislation.

Each government should also request funding in, and appropriate funding for, their budget for a national cyberbiosecurity program. Given the present cyberbiological risk to all countries, every national leader should immediately add responsibilities to reduce this risk to already funded cybersecurity and biosecurity programs and assign cyberbiosecurity oversight to a very senior-level dedicated position in their governments (e.g., the U.S. Special Assistant to the President and Senior Director for Weapons of Mass Destruction and Biodefense). Leadership should also require evaluation of cyberbiological risk to their national economies.

CONCLUSION

All countries, including the United States, face risks from many sources. Collective dependence on the Internet and electronic communications, cyber- and biological contributions to national and global economies, competitive participation in the biorevolution, and new types of combinational weapons make the need to reduce cyberbiological risk both imperative and vital. We must take the opportunity afforded to us now to eliminate this transnational security gap, before it is exploited by our enemies.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

Bajema, N. E., DiEuliis, D., Lutes, C., and Lim, Y. (2018). *The Digitization of Biology: Understanding the New Risks and Implications for Governance*. Available online at: https://wmdcenter.ndu.edu/DesktopModules/ArticleCS/Print.aspx?PortalId=97&ModuleId=44472&Article=1569559

Blue Ribbon Study Panel on Biodefense. (2015). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts–Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, DC: Blue Ribbon Study Panel on Biodefense. doi: 10.13140/RG.2.1.4407.6240

de Bono, E. (1970). *Lateral Thinking*. NewYork, NY: Harper and Row.

Findlay, T. (2006). *Verification and the BWC: Last Gasp or Signs of Life? Arms Control Today*. Available online at: https://www.armscontrol.org/act/2006_09/BWCVerification

Heus, J. J., de Pauw, E. S., Leloux, M., Morpugo, M., Hamblin, M. R., and Heger, M. (2017). Importance of intellectual property generated by biomedical research at universities and academic hospitals. *J. Clin. Transl. Res.* 3:5. doi: 10.18053/jctres.03.201702.005

Hodge, J. G. (2012). The evolution of law in biopreparedness. *Biosecurity Bioterror.* 10, 38–48. doi: 10.1089/bsp.2011.0094

Irving, M. (2017). *Artificial Evolution Aims to Create Life Out of Non-Living Matter*. New Atlas. Available online at: https://newatlas.com/recreating-evolution-test-tube/48856/

Knapp, B. (2018). *Researchers are Sounding the Alarm on Cyberbiosecurity, 5th Domain*. Available online at: https://www.fifthdomain.com/dod/2018/02/08/researchers-are-sounding-the-alarm-on-cyberbiosecurity/

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

Nakashima, E. (2018). *Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections*. Washington Post. Available online at: https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html?utm_term=.fc46e6ec038f

National Research Council. (2015). *Standards, Conformity Assessment, and Trade: Into the 21st Century*. Washington, DC: National Academies Press. doi: 10.17226/4921

Roco, M. C., and Bainbridge, W. S. (2002). Converging technologies for improving human performance: integrating from the nanoscale. *J. Nanopart. Res.* 4, 281–295. doi: 10.1023/A:1021152023349

Schatz, M. C. (2015). Biological data sciences in genome research. *Genome Res.* 25, 1417–1422. doi: 10.1101/gr.191684.115

Schneier, B. (2012). Securing medical research: a cybersecurity point of view. *Science* 336, 1527–1529. doi: 10.1126/science.1224321

Sharp, P. A., Cooney, C. L., Kastner, M. A., Lees, J., Sasisekharan, R., Yaffe, M. B., et al. (2011). The third revolution: the convergence of the life sciences, physical sciences, and engineering. Cambridge, MA: Massachusetts Institute of Technology.

Sherden, W. A. (2011). *Best Laid Plans: The Tyranny of Unintended Consequences and How to Avoid Them*. Santa Barbara, CA: Praeger.

The White House. (1998). *Memorandum for Heads of Executive Departments and Agencies (Circular No. A-119 Revised)*. Washington, DC: The White House.

US Government Accountability Office (2017). *High-Containment Laboratories: Coordinated Actions Needed to Enhance the Select Agent Program's Oversight of Hazardous Pathogens*. Washington, DC: Government Accountability Office.

Conflict of Interest Statement: The author was employed by the Blue Ribbon Study Panel on Biodefense.

frontiers in Bioengineering and Biotechnology

PERSPECTIVE
published: 29 March 2019
doi: 10.3389/fbioe.2019.00061

Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience

Daniel S. Schabacker[1], Leslie-Anne Levy[2], Nate J. Evans[1], Jennifer M. Fowler[1] and Ellen A. Dickey[1]*

[1] Argonne National Laboratory (DOE), Strategic Security Sciences Division, Lemont, IL, United States, [2] Argonne National Laboratory (DOE), Decision and Infrastructure Sciences Division, Lemont, IL, United States

The convergence of advances in biotechnology with laboratory automation, access to data, and computational biology has democratized biotechnology and accelerated the development of new therapeutics. However, increased access to biotechnology in the digital age has also introduced additional security concerns and ultimately, spawned the new discipline of cyberbiosecurity, which encompasses cybersecurity, cyber-physical security, and biosecurity considerations. With the emergence of this new discipline comes the need for a logical, repeatable, and shared approach for evaluating facility and system vulnerabilities to cyberbiosecurity threats. In this paper, we outline the foundation of an assessment framework for cyberbiosecurity, accounting for both security and resilience factors in the physical and cyber domains. This is a unique problem set, but despite the complexity of the cyberbiosecurity field in terms of operations and governance, previous experience developing and implementing physical and cyber assessments applicable to a wide spectrum of critical infrastructure sectors provides a validated point of departure for a cyberbiosecurity assessment framework. This approach proposes to integrate existing capabilities and proven methodologies from the infrastructure assessment realm (e.g., decision science, physical security, infrastructure resilience, cybersecurity) with new expertise and requirements in the cyberbiosecurity space (e.g., biotechnology, biomanufacturing, genomics) in order to forge a flexible and defensible approach to identifying and mitigating vulnerabilities. Determining where vulnerabilities reside within cyberbiosecurity business processes can help public and private sector partners create an assessment framework to identify mitigation options for consideration that are both economically and practically viable and ultimately, allow them to manage risk more effectively.

Keywords: cyberbiosecurity, vulnerability, resilience, risk, convergence, emerging, converging, technology

OPEN ACCESS

Edited by:
Diane DiEuliis, National Defense University, United States

Reviewed by:
Dana Perkins, United States Department of Health and Human Services, United States
Gerald Epstein, National Defense University, United States

****Correspondence:***
Daniel S. Schabacker
dschabacker@anl.gov

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

Received: *26 November 2018*
Accepted: *05 March 2019*
Published: *29 March 2019*

Citation:
Schabacker DS, Levy L-A, Evans NJ, Fowler JM and Dickey EA (2019) Assessing Cyberbiosecurity Vulnerabilities and Infrastructure Resilience. Front. Bioeng. Biotechnol. 7:61. doi: 10.3389/fbioe.2019.00061

INTRODUCTION

An important initial step in effectively managing risk is developing a comprehensive understanding of vulnerabilities. Stakeholders can then identify economical and practical options to mitigate vulnerabilities. Risk in the biological sciences has been managed through the implementation of standard biosecurity practices, through which vulnerabilities are (a) identified and (b) mitigated through regularly updated training, policies, and enhanced physical security. To prevent

unauthorized access to high-consequence biological agents, the U.S. Government (USG) stood up the Federal Select Agent Program (FSAP), which added extensive requirements (e.g., background checks, registration by institutions, increased oversight) for those seeking access to Biological Select Agents and Toxins (BSATs). The BSAT list is based on taxonomic classifications and includes 67 high-consequence biological agents and toxins. Advances in genetic engineering tools (e.g., CRISPR Cas 9 systems) along with the convergence of lab automation, computational biology, and access to publically available genomic databases will dramatically impact the effectiveness of the FSAP as well as other biosecurity policies and practices. It will no longer be necessary to obtain physical samples to exploit a biological agent; access to publically available genomic databases, biofoundries, lab automation, and computational biology enables the design and production of high-consequence biological agents and toxins. These biological agents may be entirely new to nature and unconstrained by taxonomic classification such as the BSAT list (Wintle et al., 2017). This new digital environment in which biological research increasingly takes place must be systematically assessed for vulnerabilities in order to effectively manage evolving risks. The new discipline of cyberbiosecurity, which includes biosecurity, cyber-physical security, and cybersecurity, directly addresses the unique risks associated with biotechnology in an increasingly digital environment (Peccoud et al., 2017; Murch et al., 2018).

In this paper, we outline the foundation of an assessment framework for cyberbiosecurity, accounting for both security and resilience factors in the physical and cyber domains. When implemented, the assessment framework will help partners identify and prioritize vulnerabilities. Importantly, the prioritization of vulnerabilities will result from a defensible, transparent, and reproducible assessment. In conjunction with an understanding of the consequences of disruption, risk mitigation strategies can be developed and considered in return-on-investment (ROI) analyses. ROIs will allow stakeholders to make informed decisions on how best to allocate limited resources for maximum impact.

While biosecurity is one of the three disciplines comprising cyberbiosecurity (e.g., biosecurity, cyber-physical security, and cybersecurity) it is well-established and will not be discussed due to space limitations.

RISK MITIGATION IN THE ERA OF CONVERGING TECHNOLOGIES

Emerging and converging technologies present new risks to security that require new methodologies for risk prioritization and mitigation.

The accelerated pace of technological advancements across nearly all scientific disciplines has been driven largely by the convergence of advancements in scientific disciplines associated with computation, networking, automation, and access to data. Convergence occurs where scientific disciplines or key enabling technologies combine with other disciplines or enabling technologies and promise new or improved capabilities. Convergence is more than the simple combination of different disciplines or technologies. It leads to synergies, adding more value through convergence (Dengg, 2018).

While converging technologies lead to fast and far-reaching improvements, they also create new security challenges and risks. We often try to address new risks with methods that were successful in the past; however, they may not be appropriate for the systemic risks posed by the increasing interconnectivity and complexity associated with converging technologies (Dengg, 2018). Additionally, with highly interconnected systems, the risk from dependencies and interdependencies must be considered. Therefore, we must take a more systemic approach to assessing and mitigating risks resulting from converging technologies.

Emerging and converging technologies have significantly increased the number of vulnerabilities to national security to levels that are untenable for the government and private sector to address in their entirety. They simply do not have the resources required to implement mitigation strategies to address risks with a low probability of occurrence and/or low consequence. Current conversations do not prioritize potential courses of action based on defensible integrated risk assessments that consider both probability and consequence in the context of converging technologies.

CYBERBIOSECURITY

The exploration of life sciences has become increasingly dependent upon internet-connected machinery and devices. Internet-dependent infrastructure is critical to computation and discovery of new avenues of research. The subsequent dependence upon technology and internet-connected devices begs the need to secure this infrastructure. For example, attackers could exploit unsecured networks and remotely manipulate biological material, creating new threats with devastating potential (Murch et al., 2018). Cyberbiosecurity aims to understand and reduce the risks associated with conducting research using advanced technologies in the bioscience field. Science exploration depends increasingly upon cloud services, cyber-physical devices, internet-connected machines, remote databases, and many other cyber-vulnerable technologies. This convergence of science and cybersecurity opens the field to a new threat landscape.

Below are two examples of vulnerabilities that may not be individually identifiable in either a biosecurity or a cybersecurity context but are only apparent when both disciplines are considered.

Bringing together advances in synthetic biology and genetic engineering with machine learning, advanced modeling, metabolic engineering and access to publically available databases containing complete genome sequences of pathogens including virulence factors will enable the design of novel high consequence biological agents completely *in silico*. Minimal laboratory infrastructure and equipment would be required. Moreover, the vast array of publically available open source tools enable execution of these processes by less experienced personnel.