Proceedings of the
Informing Science +
Information Technology
Education Conference

*An Official Publication
of the Informing Science Institute
InformingScience.org*

InformingScience.org/Publications

THE GROWING NEED FOR CYBERBIOSECURITY

Glenda Turner

Robert Morris University,
Pittsburgh, PA, USA

gxtst116@mail.rmu.edu

ABSTRACT

Aim/Purpose: This paper describes the growing need for a new transdiscipline in cyberbiosecurity as well historical challenges associated with knowledge generation and integration among contributing disciplines.

Background: Within the United States, there is an emerging call for cyberbiosecurity; however, cyberbiosecurity roles, practices and metrics have not been defined and federal agencies appear uncertain regarding how to proceed.

Methodology: Scoping study.

Contribution: This paper describes student research that is in progress. The research is aimed at providing a foundation for development of a cyberbiosecurity transdisciplinary knowledge framework.

Findings: Key contributing disciplines such as safety and security have been slow to integrate; novel methods will be required to accelerate effective cyberbiosecurity.

Recommendations for Practitioners and Researchers: Collaborate to form this new transdiscipline.

Impact on Society: This research is intended to reduce stakeholder uncertainty and accelerate formation of cyberbiosecurity as an effective transdiscipline.

Future Research: In-depth study that includes continued content review and analysis of knowledge artifacts and practices across contributing disciplines and engagement with stakeholders at different levels of government and industry to develop a cyberbiosecurity knowledge framework.

Keywords: transdiscipline, knowledge framework, cyberbiosecurity

Accepting Editor: Eli Cohen │ Received: December 5, 2018 │ Revised: February 8, 2019 │
Accepted: February 9, 2019.
Cite as: Turner, G. (2019). The Growing Need for Cyberbiosecurity. Proceedings of the Informing Science and Information Technology Education Conference, Jerusalem, Israel, pp. 207-215. Santa Rosa, CA: Informing Science Institute. https://doi.org/10.28945/4337

INTRODUCTION

Transdisciplinarity is an umbrella term for a number of evolving perspectives and approaches related to efforts conducted by practitioners from different disciplines working jointly to synthesize: to create new conceptual, theoretical, methodological, and translational innovations that integrate and move beyond discipline-specific approaches to address a common problem (Harvard, n.d.). Ertas (2010a, 2010b) focuses specifically on its collaborative knowledge generation and integration aspects and defines transdisciplinary knowledge as "a shared, common collection of knowledge from diverse disciplinary knowledge cultures (engineering, natural science, social science and humanities)" (2010b, p. 57).

Cyberbiosecurity is an emerging transdiscipline that will likely focus on (i) understanding the vulnerabilities to misuse, unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of biological and medical sciences and technologies comingled with cyber, cyber-physical, supply chain and infrastructure systems, and (ii) developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such hazards and threats as they pertain to ethics, safety, security, competitiveness and resilience (adapted from Murch, So, Buchholz, Raman, & Peccoud, 2018).

This paper provides background information on the call for cyberbiosecurity as a new transdiscipline as well as key disciplines that will potentially contribute to cyberbiosecurity. It highlights challenges associated with knowledge generation and integration that may be relevant to the emergence of a new transdiscipline, and it concludes with an outline for additional research.

METHODOLOGY

This research paper utilizes a scoping review method, which can be defined as a type of knowledge synthesis that follows a systematic approach to map evidence on a topic and identify main concepts, theories, sources, and knowledge gaps (PRISMA-SCR, 2018). Grant and Booth (2009) refer to scoping reviews as "preliminary assessments" that "cannot usually be regarded as a final output in their own right." (p. 95). This scoping review is an early phase in a planned larger grounded theory study.

FINDINGS

WHAT IS THE DEMAND FOR CYBERBIOSECURITY?

Cyberbiosecurity is a proposed new transdiscipline that has its origins in a study conducted by the American Association for the Advancement of Science and co-sponsored by the United States (US) Federal Bureau of Investigation (FBI) and the United Nations Interregional Crime and Justice Research Institute (2014); a workshop series conducted by the US National Academies of Sciences, Engineering and Medicine (NASEM) and sponsored by the US FBI (NASEM 2014, 2015, 2016); and a follow-on research project conducted by the US National Strategic Research Institute and sponsored by the US Strategic Command (Murch et al, 2018).

WHY IS CYBERBIOSECURITY CONSIDERED IMPORTANT?

Key concerns motivating the call for cyberbiosecurity as new transdiscipline include the uneven global distribution of digitized biotechnical data and associated negative impacts to the future of life, the environment, and the bioeconomy; the integrity of emerging *cyberbiophysical systems* and devices such as neuromorphic computing and 3-D bioprinting; the potential for malice such as encoding digitized DNA with malware; and increasing security risks to cyberbiophysical informatics and materials from industrial espionage (NASEM, 2014, 2015, 2016). Cyberbiophysical innovation can also include biomechatronics, which can be defined as science that aims to integrate biology, mechanics, electronics, robotics and neuroscience. (Popovic, 2019). Biomegatronics focuses on the research and design of assistive, therapeutic and diagnostic devices to compensate (partially) for the loss of human physiological functions or to enhance these functions. Recent developments include artificial organs and tissues, prosthetic limbs, orthotic systems, wearable systems for physical augmentation, physical therapy and rehabilitation, robotic surgery, and natural and synthetic sensors.

What Recommendations have been made To-date and What is Missing?

Key cyberbiosecurity recommendations to date include: training and awareness, systematics, and new policies (Kassner, 2018) as well as new standards of practice and new applications of traditional cybersecurity technologies such as data encryption to bioinformation (Bajema, DiEuliis, Lutes, & Lim, 2018). The studies to date focus only on two extremes of what promises to be an extensive spectrum: (i) broad globalization issues (NASEM, 2014, 2015, 2016) and detailed systematics within a biomanufacturing facility (Murch et al, 2018). The myriad of unaddressed topics between these two extremes includes but is not limited to (i) organizational impacts, priorities, and management approaches; (ii) the full system architecture and life cycle of cyberbio-enabled products and services; (iii) the event life cycle of cyberbio hazards and incidents; (iv) the development, sustainment, and evaluation of professional standards of practice; and (v) the evolution of regulatory regimes.

What Disciplines Might Contribute to Cyberbiosecurity as a new Transdiscipline?

Table 1 shows some of the disciplines that might contribute to cyberbiosecurity as a new transdiscipline.

Table 1. Disciplines that might contribute to cyberbiosecurity as a new transdiscipline

Discipline	Description
Risk management	The discipline concerned with coordinated activities to direct and control an organization with regard to risk, which is defined as the effect of uncertainty on objectives. Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood (ISO 31000:2018, 2018).
Biosecurity	1. The discipline concerned with strategic and integrated approaches to analyzing and managing relevant risks to human, animal and plant life and health and associated risks for the environment. (WHO, 2010). 2. The discipline concerned with establishing risk-and threat-based control measures to prevent the unauthorized access, misuse, loss, theft, diversion and intentional release of valuable biological materials, pathogens, toxins, information, expertise, equipment, technology and intellectual property that have the potential to cause harm to humans, animals, plants, the environment, public safety or national security (ABSA International, n.d.)
Biosafety	The discipline concerned with the range of measures, policies and procedures focused primarily on safe transfer, handling and use of living modified organisms for minimizing potential risks they may pose to the environment and human health (United Nations, 2003).

Discipline	Description
Bioeconomics	The discipline concerned with economic activity derived from scientific and research activity focused on biotechnology, that is, understanding mechanisms and processes at the genetic and molecular levels and applying this understanding to creating or improving industrial processes ("Bio-based economy," n.d.). Bioeconomics focuses on those parts of the economy that use renewable biological resources from land and sea – such as crops, forests, fish, animals and micro-organisms – to produce food, materials and energy (European Commission, n.d.).
Cybersecurity	The discipline concerned with the activities or processes, abilities or capabilities or states whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. It includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[es] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (National Initiative for Cybersecurity Careers and Studies, n.d.)
Cyber-physical systems security	The discipline concerned with addressing cybersecurity risks and attack surfaces in cyber-physical systems and the Internet of Things (Department of Homeland Security, n.d.). Cyber-physical systems (CPS) are engineered systems of cyber (computation and communication) and physical (sensors and actuators) components that are networked and interact in a feedback loop with the possible help of human intervention, interaction and utilization. (Ashibani & Mahmoud, 2017; National Science Foundation, n.d.).
Ethics	The discipline concerned with systematizing, defending, and recommending concepts of right and wrong behavior ("Ethics", n.d.).
Industrial biotechnology	The discipline involved in working with nature to maximize and optimize existing biochemical pathways that can be used in manufacturing. Three contributing fields of study are genomics, proteomics, and bioinformatics (bio.org., n.d.).
Synthetic biology	A new interdisciplinary area that involves the application of engineering principles to biology. It aims at the (re-)design and fabrication of biological components and systems that do not already exist in the natural world (DiEuliis, Lutes, and Giordano, 2018).

Discipline	Description
Surety	The discipline concerned with establishing positive measures to ensure there will be no accidents, incidents, or unauthorized modifications to the assets being managed and controlled (adapted from the DoD Nuclear Matters Handbook (Department of Defense, 2016).
Assurance	Within systems, the discipline concerned with establishing confidence that the system will perform as expected and only as expected. High assurance is based on mathematical evidence. See for example the US Defense Advanced Research Programs Agency (DARPA) program in High Assurance Cyber Military Systems (HACMS) (Richards, n.d.).
System safety	The discipline defined as the application of special technical and managerial skills to the systematic, *forward-looking* identification and control of hazards throughout the life cycle of a project, program, or activity (OSHA, n.d.)

What are some preliminary indicators of the state of knowledge generation and integration among contributing disciplines?

Table 2 shows some of the indicators of the state of knowledge generation and integration among contributing disciplines.

Table 2. Preliminary indicators of the state of knowledge generation and integration among contributing disciplines

Disciplines	Indicators
Biosafety and Biosecurity	Cambrosio, Limoges, Courtial, and Laville (1992) find biological safety to be "a very fragmented field, characterized by the existence of several relatively independent foci of interest, none of which has been able to structure the field into a tight network." The International Federation of Biosafety Associations (n.d.) certifies individuals in biosecurity, biorisk, and biosafety based upon an established body of knowledge.
Cybersecurity	Rashid, Danezis, Chivers, Lupu, Martin, Lewis, and Peersman (2018) document the fragmented nature of the cybersecurity body of knowledge. Mueller (2017) identifies concerns among communities engaged in Internet governance that cybersecurity is overwhelming other aspects of Internet governance and that the cybersecurity community has a geopolitical and national security focus that is at odds with the Internet's transnational and societal focus.
System Safety	Yamamoto (2014) finds that international standards communities have been both slow and uneven in their embrace of innovations for safety critical software.
Integration of safety and security	Foote (2015) observes that "the concept of integrated security and safety has been around for some time, and it is interesting to note the lead taken by the UK's Office for Nuclear Regulation recently in the integration of its safety and security regulatory organisation. However, the delivery of integrated

	safety and security by industry has been slow, predominantly because of the different approaches taken by the two sets of practitioners, and the higher levels of security clearance required for some of the more sensitive activities. Furthermore, security has tended to be more prescriptive than the risk-based practice of safety and also communication around security tends to be on a need-to-know basis whereas safety emphasises widespread, open communication.
Safety and Security in Organizational Governance	In 2015, in response to a number of biosafety incidents at the US Centers for Disease Control and Prevention (CDC), the CDC Advisory Committee to the Director found that "leadership commitment toward safety has been inconsistent and insufficient at multiple levels." Further, "safety, including lab safety, is viewed by many as something separate from and outside the primary missions of public health and research. Safety is not integrated into strategic planning and is not currently part of the CDC culture, enterprise-wide" (CDC Advisory Committee, 2015). In 2015, in contrast to prior year surveys, the Georgia Institute of Technology survey on cybersecurity governance "shows the needle has moved, and … [corporate] boards are now undertaking key oversight activities related to governance of cybersecurity" (Westby, 2015).

What Transdisciplinary Principles and Characteristics might be Important to Emphasize and Encode Early Within Cyberbiosecurity?

Table 3 lists some of the important principles and characteristics that are important to emphasize *and* encode early within cyberbiosecurity.

Table 3. Trandisciplinary principles and characteristics potentially important for cyberbiosecurity

Principles and characteristics	Rationale
Systemic thought and systems perspectives	"Complex problems need an epistemological approach that does justice to the complexity of reality from which systems phenomena emanate" (Hofkirchner, 2017, p .4). "Systems theories provide an ontology in which complex problems are pictured as complex because they take part in an overall interconnectedness of processes and structures that are constituted by self-organising real-world systems. Those systems bring about evolution and nestedness as emergent features of reality" (p. 7).
The inclusion of societal voices in cyberbiosecurity debates	"Transdisciplinary research is research that includes cooperation within the scientific community and a debate between research and the society at large. Transdisciplinary research therefore transgresses boundaries between scientific disciplines and between science and other societal fields and includes deliberation about facts, practices and values" (Hadorn et al., 2008)

Prevention through Design (PtD)	Prevention through Design began as a US National Institute of Occupational Health and Safety (NIOSH) initiative to mitigate hazards by designing them out. “PtD is a shared concept crossing many diverse disciplines including; agriculture, forestry and fishing; construction; health care and social assistance; manufacturing; mining; services; transportation, warehousing, and utilities; and wholesale and retail trade. …In summary, Prevention through Design is a transdisciplinary process that involves many transnational and transcultural issues” (Ertas, 2010b).
Evaluation efforts that emphasize the quality of synthesis and integration	The US National Academies of Science has recognized that synthesis and integration are core to the definition of inter- or transdisciplinary research. “Interdisciplinary research (IDR) is a mode of research by teams of individuals that integrates information, data, techniques, tools, perspectives, concepts, and/or theories from two or more disciplines or bodies of specialized knowledge to advance fundamental understanding or to solve problems whose solutions are beyond the scope of a single discipline or area of research practice.” (NASEM, 2005). Pohl et al. (2010) extend these concepts to evaluation of research proposals. For cyberbiosecurity, emphasis on these qualities needs to be further extended beyond research evaluation into evaluations related to design, engineering, operations, and governance.

Conclusions

This paper describes student research that is in progress. The paper explores the growing need for cyberbiosecurity. It conceptualizes cyberbiosecurity as an emerging transdiscipline and identifies existing disciplines that will potentially contribute to the new transdiscipline. It explores the state of knowledge generation and integration within and among potential contributing disciplines, and it identifies key principles and characteristics of transdisciplinarity that will be important to encode early in cyberbiosecurity. The paper’s preliminary findings have been developed to support a planned grounded theory study focused on the development of a cyberbiosecurity knowledge framework.

References

ABSA International (n.d.) The Association for Biosafety and Biosecurity. Retrieved from https://absa.org

American Association for the Advancement of Science, Federal Bureau of Investigation and United Nations Interregional Crime, and Justice Research Institute. (2014). *National and transnational implication of security of big data in the life sciences*. Washington, DC: American Association for the Advancement of Science.

Ashibani, Y., & Mahmoud, Q. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81-97. https://doi.org/10.1016/j.cose.2017.04.005

Bajema, N. E., DiEuliis, D., Lutes, C., & Lim, Y-B. (2018). *The digitization of biology: Understanding the new risks and implications for governance*. Washington, DC: National Defense University. Retrieved from https://wmdcenter.ndu.edu/Portals/97/Documents/Publications/EC%20research%20paper%20no%203%20-%20DiEuliis%20Bajema%20Lim%20-%20FINAL.pdf?ver=2018-07-09-104517-157

Bio-based economy. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/wiki/Biobased_economy

Cambrosio, A., Limoges, C., Courtial, J.-P., & Laville, F. (1992). Historical scientometrics? Mapping over 70 years of biological safety research with coword analysis, *Scientometrics* 27(2). DOI: https://doi.org/10.1007/BF02016546

CDC Advisory Committee. (2015). *Minutes for US Centers for Disease Control and Prevention*, Retrieved from https://www.cdc.gov/

Department of Defense (DoD). (2016). *Nuclear matters handbook, 2016*. Retrieved from https://www.acq.osd.mil/ncbdp/nm/nmhb/index.htm

Department of Homeland Security (DHS). (n.d.) *Cyber-physical systems security (CPSSEC)*. Retrieved from https://www.dhs.gov/science-and-technology/csd-cpssec#

DiEuliis, D., Lutes, C. & Giordano, J. (2018). Biodata risks and synthetic biology: A critical juncture. *Journal of Bioterrorism & Biodefense*. https://doi.org/10.4172/2157-2526.1000159

Ertas, A. (2010a). Transdisciplinarity: Design, process and sustainability. *Transdisciplinary Journal of Engineering and Science*. 1(1), 30-48.

Ertas, A (2010b). Understanding of transdiscipline and transdisciplinary process. *Transdisciplinary Journal of Engineering & Science*. 1(1), 55-73.

Ethics. (n.d.). *Internet encyclopedia of philosophy*. Retrieved from https://www.iep.utm.edu/

European Commission. (n.d.). *What is the bioeconomy*? Retrieved from https://ec.europa.eu/research/bioeconomy/index.cfm

Foote, K. (2015). Safe and secure? The integration of safety and security. *Riskworld, 28*, 4. Warrington, UK. Retrieved from https://www.risktec.tuv.com/wp-content/uploads/2018/09/safe-and-secure-the-integration-of-safety-and-security.pdf

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information and Libraries Journal, 26*, 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Hadorn, H. G., Biber-Klemm, S., Grossenbacher-Mansuy,W., Hirsch Hadorn, G., Joye, D., Pohl, C., Wiesmann, U., & Zemp, E. (2008). *Handbook of transdisciplinary research, enhancing transdisciplinary research: A synthesis in fifteen propositions*. Chapter 29, p. 435. https://doi.org/10.1007/978-1-4020-6699-3_29

Harvard. (n.d.). *Harvard transdisciplinary research in energetics and cancer center*. School of Public Health. Retrieved from https://www.hsph.harvard.edu/trec/about-us/definitions/

Hofkirchner, W. (2017). Transdisciplinarity needs systemism. *Systems* 2017, *5*, 15. https://doi.org/10.3390/systems5010015

International Federation of Biosafety Associations (IFBA). (n.d.).. Retrieved from https://www.internationalbiosafety.org

ISO 31000:2018. (2018) *Risk management – guidelines*. International Organization for Standardization. Retrieved from https://www.iso.org/standard/65694.html

Kassner, M. (2018). *How to manage cyberbiosecurity risks before a malware attack strikes*. Retrieved from https://www.techrepublic.com/article/how-to-manage-cyberbiosecurity-risks-before-a-malware-attack-strikes/

Mueller, M. (2017). Is cybersecurity eating internet governance? Causes and consequences of alternative framings. *Digital Policy, Regulation and Governance*, *19*(6), 415-428. https://doi.org/10.1108/dprg-05-2017-0025

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

National Academies of Sciences, Engineering and Medicine (NASEM). (2005). *Facilitating interdisciplinary research*. The National Academies Press. https://doi.org/10.17226/11153

National Academies of Sciences, Engineering and Medicine (NASEM). (2014). *Meeting recap, workshop – convergence: Safeguarding technology in the bioeconomy*. Organized by the Board on Chemical Sciences and Technology and the Board on Life Sciences, Washington, DC.

National Academies of Sciences, Engineering and Medicine (NASEM). (2015). *Meeting recap, safeguarding the bioeconomy: Applications and implications of emerging science*. Organized by Board on Chemical Sciences and Technology, Washington, DC.

National Academies of Sciences, Engineering and Medicine (NASEM). (2016). *Meeting recap, safeguarding the bioeconomy iii: Securing life sciences data.* Organized by the Board on Life Sciences and Board on Chemical Sciences and Technology. Washington, DC.

National Initiative for Cybersecurity Careers and Studies (NICCS). (n.d.). Retrieved from https://niccs.us-cert.gov/about-niccs/glossary

National Science Foundation (NSF) (n.d.). *Cyber-physical systems*. Retrieved from https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286

OSHA (n.d.) *System safety*. US Occupational Safety and Health Academy. Retrieved from https://www.oshatrain.org/notes/2bnotes02.html

Pohl, C., Perrig-Chiello, P., Butz, B., Hirsch Hadorn, G., Joye, D., Lawrence, R., ... & Wastl-Walter, D. (2011). Questions to evaluate inter-and transdisciplinary research proposals. *Network for Transdisciplinary Research (td-net) of the Swiss Academies of Arts and Sciences, Bern*, 23.

Popovic, M. (2019). *Biomegatronics* (1st ed.). Cambridge, MA. Academic Press

PRISMA. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine*. https://doi.org/10.7326/M18-0850

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, *16*(3), 96-102. https://doi.org/10.1109/msp.2018.2701150

Richards, R. (n.d.). *High-assurance cyber military systems* (hacms). https://doi.org/10.1145/2402676.2402695

United Nations (UN). (2003). *Biosafety and the environment: An introduction to the cartagena protocol on biosafety*. Montreal, Quebec, Canada. Retrieved from https://www.cbd.int/doc/press/presskits/bs/cpbs-unep-cbd-en.pdf

Westby, J. R. (2015). *Governance of gybersecurity: 2015 Report*. GTISC. Retrieved from https://globalcyberrisk.com/wp-content/uploads/2012/08/GTISC-GOVERNANCE-RPT-2015-v15.pdf

World Health Organization (WHO). (2010). *INFOSAN Information Note No. 1/2010 – Biosecurity*. Retrieved from http://www.who.int/foodsafety/fs_management/No_01_Biosecurity_Mar10_en.pdf

Yamamoto, S. (2014). A knowledge integration approach of safety-critical software development and operation based on the method architecture. Proceedings of the *Knowledge-Based and Intelligent Information & Engineering Systems 18th Annual Conference, KES-2014 Gdynia, Poland*, pp. 1718-1727. https://doi.org/10.1016/j.procs.2014.08.265

Biography

Glenda Turner is a doctoral student in Information Systems and Communications at Robert Morris University in Pittsburgh, PA, USA. Ms. Turner directs a portfolio of engineering research at a non-profit organization focusing on safety and security. She has an abiding interest in the history of science and technology, and her recent focus has been the advent of big science in the United States and its relationship to World War II and nuclear, biological, and chemical defense.