# UNDERSTANDING THE LANDSCAPE OF CYBERBIOSECURITY FOR INTEGRATIVE EDUCATIONAL PROGRAMMING


**Collection Review**

Samson O. Adeoye[1,*], Feras Batarseh[2], Anne M. Brown[3], Eric K. Kaufman[1]

[1] Agricultural, Leadership, and Community Education, Virginia Tech, Blacksburg, Virginia, USA.
[2] Biological Systems Engineering, Virginia Tech, Blacksburg, Virginia, USA.
[3] Research and Informatics, University Libraries, Virginia Tech, Blacksburg, Virginia, USA.
[*] Correspondence: sadeoye@vt.edu, samadeoyeola@gmail.com

## HIGHLIGHTS

- Alignment of terminology and community building are crucial in cyberbiosecurity.
- Agriculture and life sciences in a digital age present unconventional challenges.
- Data and digital literacy are baseline skills for integrative cyberbiosecurity education programming.
- Cyberbiosecurity education framework offers a foundation for intentional, integrative programming efforts.

**ABSTRACT.** *As an emerging and interdisciplinary field at the nexus of digital technologies and agriculture and life sciences (ALS), the integration of cyberbiosecurity education for professional training and skills development remains challenging. Educational practices and related workforce development efforts associated with cyberbiosecurity may be best generalized as pseudo-shadow education, occurring outside standardized practice and lacking known 'best practice' to mimic. The current state of cyberbiosecurity education reflects a lack of sequenced and developed knowledge, values, judgments, and ways of thinking, which serve as windows into the underlying cultures of a disciplinary field. Coupled with this gap, the continuous deployment and convergence of information technology (IT) and operational technology (OT) within ALS creates new vulnerabilities that are unfamiliar to the workforce. These vulnerabilities expose critical ALS infrastructures to cyber-attacks and terrorism and hold significant consequences for the bioeconomy. Securing the bioeconomy and preventing negative multiplier effects in other related sectors depend on adequate cyberbiosecurity education programming and workforce development. This exploratory report of current realities and future prospects provides insights into integrative cyberbiosecurity education programming for workforce development. The study explicates underlying concerns to be addressed in developing integrative cyberbiosecurity education for professionals in agriculture and life sciences and suggests an expandable framework to facilitate workforce development programming. Concerns to address regarding the creation of educational programming in cyberbiosecurity include alignment in definition, cross-boundary community building, the peculiar dynamics of the cyberbiosecurity threat landscape, and baseline requirements for cyberbiosecurity education and practice.*

***Keywords.*** *Agriculture and life sciences, Bioeconomy, Cyberbiosecurity, Education and workforce development, Threat landscape.*

Cyberbiosecurity is an emerging field intersecting the domain areas of digital technologies and agriculture and life sciences (ALS) (Murch et al., 2018; Richardson et al., 2019a). Broader definitions of cyberbiosecurity have emerged as more research endeavors are geared toward deepening the understanding of this emergent and crucial field. Duncan et al. (2019) and Schabacker et al. (2019) further broadened the definition by considering the interconnection of cybersecurity, cyber-physical security, and biosecurity. Mueller (2021) emphasized the nexus of cybersecurity, biosecurity, and biosafety in their explanation of cyberbiosecurity. The different lenses and sub-categories of cyberbiosecurity are not far-fetched. The field is nascent (see Murch and DiEulius (2019), as well as Greenbaum (2023), for a collection of cyberbiosecurity studies). Understandably so, there is not yet a universally agreed-upon definition of cyberbiosecurity or any targeted educational framework for workforce training (Murch, 2023).

Notwithstanding, existing perspectives to cyberbiosecurity indicate a transcendence away from traditional cyberattacks and demands that addressing cyber-related security challenges can no longer be approached as though they were merely an IT concern (Greenbaum, 2023). The different, multiple points of intersections, whether at the cyberspace

Submitted for review on 18 July 2023 as manuscript number EOPD 15739; approved for publication as a Review Article and as part of the Cyberbiosecurity: Securing Water and Agricultural Systems Collection by Associate Editor Dr. Robert Gustafson and Community Editor Dr. Monica Gray of the Education, Outreach, & Professional Development Community of ASABE on 26 September 2023.

  ISSN 2769-3295 https://doi.org/10.13031/ja.15739 

level or the physical systems that enable connections or biosafety and biosecurity, are potential vulnerabilities that have been created by digitized processes in ALS operational systems (Duncan et al., 2019; Mueller, 2021). Figures 1 and 2 detail these intersections across chains of activities and industries, and highlight points of possible vulnerabilities and breaches. These vulnerabilities and breaches at different, interconnected levels of cybersecurity, bio security and safety, cyber-physical security, and biotechnology, and the integrative know-how required to safeguard critical infrastructures, are what distinguish cyberbiosecurity from cybersecurity or biosecurity. Cyberbiosecurity seeks to address complex overlaps that go beyond a siloed and reductionist approach of merely applying cyber tools to biological systems or vice versa.

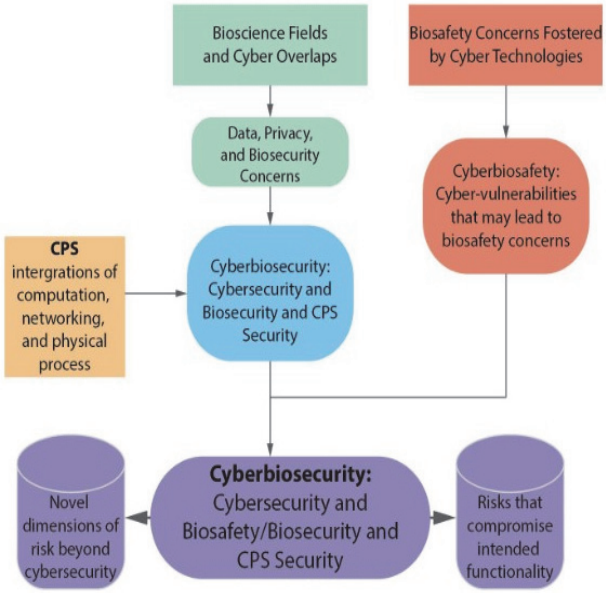


**Figure 1. Emergence and Scope of Cyberbiosecurity. Adapted from "Facing the 2020 pandemic: What does cyberbiosecurity want us to know safeguard the future?" by Mueller (2021), *Biosafety and Health.* http://doi.org/10.1016/j.bsheal.2020.09.007**

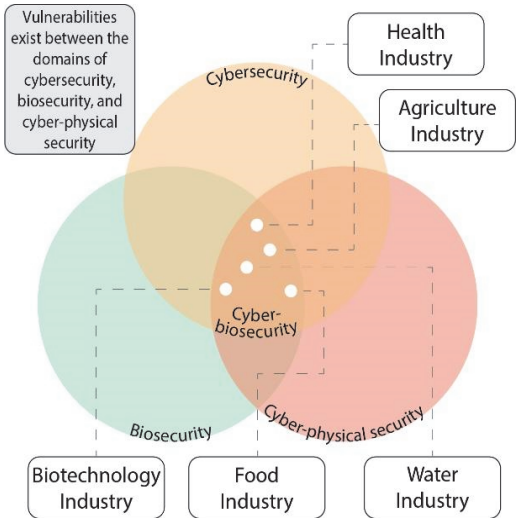


**Figure 2. Overlapping Functions and Domains of Cyberbiosecurity. Adapted from "Cyberbiosecurity: A new perspective on protecting U.S. Food and Agricultural system" by Duncan et al. (2019), *Frontiers in Bioengineering and Biotechnology*. https://doi.org/10.3389/fbioe.2019.00063**

Vulnerabilities create loopholes that favor conducive threat environments for threat actors and cyberattackers to capitalize on, gain access to, and disrupt the normal functioning of operational systems. In agriculture, disruptions to critical data and infrastructure pose danger to sustainable food production and supply and hamper the bioeconomy significantly (Chi et al., 2017; Salam, 2020; Titus et al., 2023). As a sector that has been more heavily invested in mechanical devices than technology, the realities of digital transformation in agriculture call for critical attention. With technology-enhancing precision agriculture, significant improvements in the efficiency of water use for irrigation, agrochemical application, seed and other planting material use, and overall output improvement are now much more remarkable. The attendant security challenges and potentially devastating outcomes raise concern regarding the intended and unintended consequences of agricultural digitization. Demonstrating the need for cyberbiosecurity in modern, advanced agriculture, Stephen et al. (2023) raise consciousness on critical vulnerabilities that threat actors can exploit to disrupt a farm's operations (fig. 3).

As shown in figure 3, "A" indicates a point of vulnerability where cyberattacks on the electrical power grids could interfere with farm operations that require electricity, causing a significant breakdown of critical operations such as feeding and milking activities in a dairy farm and storage systems and controlled environment collapse. Point "B" is an example of possible cyberattacks, including minimum perturbation attacks, on drones used on farms. Such "attacks could result in the deterioration of the quality of the soil, increasing the difficulty of producing and maintaining a large quantity of agricultural goods" (Stephen et al., 2023). Also, vulnerabilities exist at the agricultural sensors and climate controls of storage silos ("C"), such as ransomware threats. Point "D" highlights potential cyberattacks on water distribution and irrigation systems (Batarseh and Kulkarni, 2023). Point "E" raises awareness that "cyber attackers could target agricultural sensors tracking information regarding: the amount of sunlight received, amount of humidity, compression and density of soil, climate of environment surrounding, soil air penetration, farming activity conducted on soil, and similar data regarding the soil" (Stephen et al., 2023). The consequences of cyberattacks are immense. Point "F"

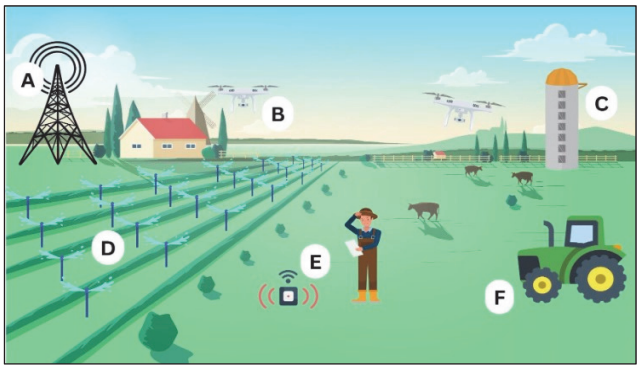


**Figure 3. Possible Cyberbiosecurity Vulnerabilities in Modern Agriculture. From "Implications of cyberbiosecurity in advanced agriculture," by Stephen et al. (2023), *Proceedings of the 18th International Conf. on Cyber Warfare and Security* (https://doi.org/10.34190/iccws.18.1.995). Reprinted with permission.**

indicates the unpalatable effect when farm machinery, tools, or equipment are directly targeted, making farming and agriculture become even more difficult. This complicates the already tedious nature of agricultural operations, and the situation is exacerbated when applied to the larger supply chain inherent in ALS.

The nuances of cyberbiosecurity and its immature state of educational endeavors make research to develop adequate educational and training practices important. Challenges in crafting well-targeted education programming span across issues, including the emergent nature of cyberbiosecurity, difficulty to identify who a cyberbiosecurity professional is, or scarcity of existing educational programs specific to cyberbiosecurity (rather than only cybersecurity or biosecurity). Moreover, the convergence of disciplines that comprise cyberbiosecurity is not explicit. All of these suggest the current state of cyberbiosecurity education may be best understood as shadow education (Zhang and Bray, 2020). Shadow education generally refers to educational opportunities outside formal schooling. Educational practices and related workforce development skills associated with cyberbiosecurity appear to be hidden in the shadows of more established programs such as computer science, engineering, and ALS, albeit in non-integrative forms. This makes it challenging to develop programming opportunities that comprehensively address specific knowledge gaps in cyberbiosecurity. The concept of shadow education is described later in this article.

The goal of this study is to illuminate the current state of cyberbiosecurity education to guide future educational program directions for professionals interfacing with emergent concerns at the intersection of biological and digital processes. We explored current cyberbiosecurity literature and evidence and elaborate on the polylithic nature of cyberbiosecurity, the need for alignments in terminology and community building, the cyberbiosecurity threat landscape, data and digital skills, and workforce development.

## Multidisciplinary, Interdisciplinary, or Transdisciplinary Educational Programming?

Cyberbiosecurity is a convergence domain field of disciplinary areas intersecting digital technology and ALS that seeks to address concerns related to agricultural/biological data and systems protection and security (Drape and Murch, 2022). Given the broadness of technology and ALS, these two domains confluence different disciplines within themselves. To sufficiently study cyberbiosecurity requires careful consideration of the many different intersecting disciplines involved. The polylithic nature of cyberbiosecurity reiterates the importance of education as "a complex world with many styles, values, and philosophies" (Glebe, 2020). Approaching cyberbiosecurity education programming through the lenses of multiple disciplines can help to simplify the complex phenomenon and provide workable means of integrating the various parts into a comprehensive framework for training and developing the workforce that interface with the real world of technology and ALS convergence. This approach promises holistic understanding, different perspectives, innovative solutions, an understanding of the real world, and collaboration skills (Briguglio and Moncada, 2019; Glebe, 2020) for addressing the challenges of cyberbiosecurity in related industries.

Understanding the way knowledge from different disciplines are harnessed and communicated is important. This notion is central to the distinctions in the concepts of multidisciplinarity, interdisciplinarity, and transdisciplinarity in educational programming. Choi and Pak (2006) put these terms in perspective and flatten the common definition ambiguities:

> Multidisciplinarity draws on knowledge from different disciplines but stays within their boundaries. Interdisciplinarity analyzes, synthesizes and harmonizes links between disciplines into a coordinated and coherent whole. Transdisciplinarity integrates the natural, social and health [and related sciences] sciences in a humanities context, and transcends their traditional boundaries.

The multiple-disciplinary approach sought in cyberbiosecurity education is a coordinated knowledge that transcends staying within a disciplinary boundary but analyzes, integrates, and harmonizes the links across relevant disciplines. This is particularly important as merely 'staying within boundaries' and the unwillingness to cooperate is one of the major challenges confronting cyberbiosecurity efforts (Richardson et al., 2019a). While transdisciplinarity is desirable in a field such as cyberbiosecurity, it is our belief that transdisciplinarity is a much longer-term pursuit that will benefit from a thorough understanding of the interdisciplinarity dimension. Hence, this paper is delimited to understanding the interdisciplinary dimensions of cyberbiosecurity for building a realistic and integrated community of professionals working to protect and secure ALS critical infrastructures.

Kaufman et al. (2023) demonstrate the interdisciplinarity potential by problematizing the cyberattack on the Oldsmar water utility in Florida, United States, in a teaching case that allows learners to tackle cyberbiosecurity through different but collaborative disciplinary lenses. From a more technical dimension, emphasizing the importance of deep learning, researchers are analyzing artificial intelligence (AI)-based approaches for detecting advanced persistent threats (APT), where threat actors can launch attacks with little or no chance of being noticed, in water distribution systems (Kulkarni et al., 2023; Sikder et al., 2023; Sobien et al., 2023). The authors' in-depth study of deep learning algorithms and AI assurance reemphasize the multidimensional nature of cyberbiosecurity issues. However, more deliberate efforts are needed to create cyberbiosecurity education that intentionally focus on integrative training opportunities for professionals, including farmers, producers, supply chain experts, and operators of ALS-related systems such as irrigation, water distribution systems, and smart farms.

The benefits of interdisciplinary education are replete in literature. However, many considerations seem to remain untapped with regard to maximizing the inescapable challenges that come with interdisciplinarity in educational design and learning (Yaman et al., 2005; Blair, 2012; Elhassan, 2012; Schreurs, 2015). These concerns range from educators to learners and can threaten potential educational outcomes. In what they called the "dark side" of interdisciplinary approaches, Schreurs (2015) identified some of these

challenges as time pressure, efficiency, personal and professional trust and mistrust, clinging to familiar ways, resistance to change, and a generalist approach. These dark sides relate closely to some of the prominent challenges in addressing cyberbiosecurity issues. For example, Richardson et al. (2019a) and Cooper (2015) emphasized trust and mistrust issues and the reluctance among ALS and IT professionals and stakeholders to collaborate toward a common cause.

This correspondingly reinforces the resistance to change and nurtures the tendency to cling to familiar ways of doing things, complicating the time pressure inherent in tackling a challenge as complex as cyberbiosecurity. Unfortunately, neither of the two broad domains (agro/bio nor cyber) has the agency to individually protect and secure the critical infrastructures at the convergence domain of cyberbiosecurity (Richardson et al., 2019a). Incorporating stakeholders' perspectives to harness existing information in cyberbiosecurity education and offering insights for integrative interdisciplinary educational programming is needed. This will promote opportunities for education and extension program designs to equip farmers, producers, supply chain experts, etc. who are unfamiliar with cyber issues to tackle emerging concerns in ALS in a digital world. Particularly, farmers may not possess adequate knowledge of cyberbiosecurity and may rely on extension or advisory services to facilitate information and operational decisions related to adequately running farms or agribusinesses and securing them from unwanted interferences. Data breaches and theft or systems disruptions with potential systems damage and intellectual property and financial losses occasioned by limited skills in handling cyberbiosecurity incidents makes the reliance on such external sources worthwhile. The challenge here is that traditional extension education and programming are no longer effective in addressing new challenges in this digital age (Ahmadpour and Mirdamadi, 2010). To thrive amidst the perilousness befallen the ALS sector, educators have a mandate to simultaneously reconsider extension service and practice viz-a-vis contemporary cyberbiosecurity issues and integrate multiple disciplinary perspectives into programming efforts.

## Agriculture and Life Sciences in a Digital Age

The burgeoning world population and the growing needs to sustain it have made technological advances in ALS pertinent. However, ALS in a digital age presents new realities that require urgent attention to safeguard the bioeconomy. Duncan et al. (2019) put this succinctly:

> The food and agriculture sectors are immensely diverse, and they require advanced technologies and efficiencies that rely on computer technologies, big data, cloud-based data storage, and internet accessibility. There is a *critical* need to safeguard the cyber biosecurity of our bio economy, but currently protections are minimal and do not broadly exist across the food and agricultural system.

Advances in food and agriculture, genetics and breeding, regenerative biology, plant-derived vaccines, etcetera, continue to leverage possibilities in cyber technologies (Duncan et al., 2019). These advances have marked impacts on the ways food, water, drugs, vaccines, etcetera, are produced, processed, and supplied (Jung et al., 2021; Monteiro and Barata, 2021; Ramirez-Asis et al., 2022). The false perception that ALS is alienated from the digital world is a denial of the reality that has befallen us all. Indeed, ALS is not familiar with some of the contemporary challenges of the digital age but are not exonerated from its cause and consequence. Past technological revolutions in agriculture, for example, were farm-based, but the digital revolution disrupts this convention as it sparks changes and concerns along multiple nodes of the food and agricultural value chains (Schroeder et al., 2021). This suggests why cyber challenges of this new and unstoppable world of digital technology are being grappled within ALS without much success.

There is an urgent need for understanding how ALS is positioned to navigate the burgeoning challenges accompanying digitization toward securing the sector's critical infrastructure. This begins with understanding the point of convergence of the distinct fields of ALS and digital technology and the benefits of the differential perspectives of relevant disciplinary areas when pooled together. The point of convergence also depicts the point of collaboration and community building (refer to figs. 1, 2, and 3). While biosafety and biosecurity have provided risk management measures within the life sciences, they are deficient in preparing and handling cyber risks and exposures (Berger and Schneck, 2019; Duncan et al., 2019). And though cybersecurity intends to provide protection against data theft and unauthorized alterations, compromised systems allow unethical access to computer programs (Rodríguez et al., 2021), falling short of managing biological risks. Cyberbiosecurity seeks to bridge this gap, harmonize conceptual framings, and crystalize security networks at points of convergence and vulnerabilities (Murch, 2023).

Starting from what we know, accepting our reality, and proceeding toward the unknown is an old philosophy of knowledge creation that holds value for learning and understanding cyberbiosecurity. It remains unclear how researchers, educators, and practitioners conceive cyberbiosecurity and are open to the new learning and collaboration that it brings – all of which "triggers different levels of comfort and discomfort" in every stakeholder (Freeth and Caniglia, 2020). Cyberbiosecurity is typical of an interdisciplinary field, where interdisciplinary stakeholders (researchers, educators, and practitioners) cannot be assumed to know how to collaborate (Freeth and Caniglia, 2020). The challenges for ALS in a digital age hinge on interdisciplinarity and collaboration, and have different implications for and responses from cyberbiosecurity stakeholders depending on the nature of the threat landscape.

### *Cyberbiosecurity Threat Landscape*

Since, unlike previous technological revolutions, the digital revolution is sparking changes and concerns along multiple nodes of ALS, supply chains, and the bioeconomy in general, understanding and developing integrative cyberbiosecurity education programs need to begin with unraveling the multiple concerns and perspectives of professionals along the different nodes (DiEuliis, 2023). Cyber incidents within the ALS industry, particularly since 2020, offer opportunities for appreciating the cyberbiosecurity threat

landscape. This period is important for understanding cyberbiosecurity as cyber incidents in food and agriculture were reported to increase to 607% in 2020 alone and have continued to gain momentum (Arntz, 2021; FBI, 2021; Creasey, 2023). The scale and diversity of these attacks continue to be reported in food and agriculture and water and wastewater systems, indicating a deliberate target on the bioeconomy (Cybersecurity and Infrastructure Security Agency, 2021; Kovacs, 2021; FBI et al., 2022; National Sanitation Foundation, 2022; Jones, 2023). The remote bricking, by some unknown Ukrainians, of reportedly seized Ukrainian tractors by Russian soldiers in 2022 tells a significant story of the possibilities and vulnerabilities in modern ALS in a digital age (Brumfield, 2022). While some celebrate this bricking as a 'win' for the Ukrainians who are fighting to defend their country, the incident further opens the discussion on the ethical and legal perspectives of cybersecurity and the potential dangers food and agriculture systems may be exposed to in a possible cyberwarfare. If a tractor is hackable for a good or bad reason, will it not pose risks to food production and supply mechanisms and the fight to end hunger and malnutrition? Are farmers, producers, and other practitioners equipped with the relevant knowledge and skills to navigate these difficult times and safeguard their businesses, as well as our collective food system and bioeconomy?

Many of the early cyberattacks on agriculture are related to ransomware (FBI, 2021, 2022), suggesting money is the motivation of the cyberattackers. Although that is not sufficient for security analysis, a combined understanding of the type of threat actor and their capability and infrastructure, as well as targeted victims, is important for judging attack intent as well as crystalizing defense mechanisms (see Caltagirone et al., 2013, for a deep dive into the diamond model of intrusion analysis). Understanding cyberbiosecurity analysis is uniquely complex because of the heterogeneous nature of technology, data, and information systems used in ALS, including a variety of sensor networks, remote sensing, drones, management software, etc., many of which may be present in a given ALS organization at a given time (Cheein and Carelli, 2013; Chi et al., 2017; Sontowski et al., 2020). The Oldsmar, Florida, water treatment plant attack in 2021 deviates from a ransomware incident, where attackers sought to poison the city's water by increasing the amount of water treatment chemical (sodium hydroxide) from 100 parts per million to 11,100 parts per million. Some reports have identified the Oldsmar water incident as an advanced persistent threat (APT). In an APT, threat actors, sometimes state-sponsored, stealthily gain access to computer networks and systems, with very little chance of being detected, to steal information, alter the normal functioning of critical operational systems, or damage IT systems (Cybersecurity and Infrastructure Security Agency, n.d.). Practitioners are confronted with complex adaptive challenges that challenge their current knowledge and require them to change the way they think and act. The design and implementation of effective cyberbiosecurity measures and strategies as well as education programming will vary across the agriculture, food, and life science supply chains.

Farmers in the United States are increasingly using digital, smart technology (especially smartphones and other mobile computing devices) in their farming operations. In 2021, 82% of farmers had access to the internet, and 77% and 67% had a smartphone and desktop/laptop computers, respectively (USDA NASS, 2021). While farmers continue to adopt and enjoy the benefits of digital technology in improving and increasing work efficiency and effectiveness, many are not aware of the accompanying dangers and inherent risks associated with digitization and connectivity to cyber-physical systems and cyberspace (Drape et al., 2021; Baker et al., 2022; Russel, 2022). This knowledge gap poses potential challenges in protecting and securing agricultural information and operational systems from unwanted and unwarranted intrusions (Spaulding and Wolf, 2018; Nikander et al., 2020; Russell, 2022). As a consequence, criminal actors will continue to succeed at exploiting ALS systems for financial gain and espionage. Even more concerning is the fact that data breaches and operations disruption in ALS systems have multiplier effects in other sectors like health, energy, and the environment.

## Nebulous Definition: How Can We Better Define Cyberbiosecurity?

What is cyberbiosecurity? We began this paper by defining cyberbiosecurity and highlighting some of its nuances. Like other emergent areas of study, and even in established fields, definitions keep evolving with the discovery of new knowledge. A definition determines the foundation and path to the development of a new field as well as serving as a basis for complex problem identification and systematic, rigorous research undertaking (Bauman et al., 2013). When definitions are nebulous, they can stall progress in research and advancement of a field. Looking at cyberbiosecurity and the relevant interconnections, a clear and precise definition needs to meet the needs of at least three key stakeholder communities – education, research, and industry.

These stakeholder groups play a significant role in activities at the intersection of information technology (IT) and operational technology (OT) within ALS. Achieving alignment in definitions that consciously addresses their respective concerns may bring us closer to a universally acceptable definition or framework of cyberbiosecurity. Table 1 shows a non-exhaustive list of the growing definitions of cyberbiosecurity. This study is not about particular wordings of a definition; it calls on education programmers to be conscious of key stakeholders and constructs and make sure to incorporate relevant concerns in the operationalization of cyberbiosecurity. Beyond specific wordings of terminologies, we preference an alignment of frameworks and common language and understanding.

Qualitative findings from a related survey (Adeoye et al., 2023) indicate that the definition of cyberbiosecurity is nebulous.

> *I'm not familiar with any courses specific to cyberbiosecurity – the definition of this term is sufficiently nebulous that I'm not sure where I'd draw a line between existing cybersecurity tools and techniques and just applying those to biology-specific techniques (e.g., securing the firmware on a liquid handler – is that 'cyberbiosecurity' or just cybersecurity?).*

**Table 1. Defining Cyberbiosecurity.**

| Definition | Source |
|---|---|
| "Cyberbiosecurity is an emerging discipline for protecting life sciences data, functions and operations (or infrastructure), and the bio economy." | Duncan et al. (2019) |
| "Cyberbiosecurity is an emerging discipline encompassing vulnerabilities and corrective measures needed to address the unique risks existing at the intersection of cybertechnology and biotechnology." | Mantle et al. (2019) |
| "Cyberbiosecurity is highly cross-disciplinary and will benefit from integrating existing capabilities and proven methodologies from a wide range of fields (e.g., security engineering, physical security and privacy, infrastructure resilience, and security psychology) with requirements from the life-science realm." "Cyberbiosecurity is an evolving paradigm that points to new gaps and risks fostered by modern biotechnologies' cyber-overlaps." | Mueller (2021) |
| Cyberbiosecurity is 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." | Murch et al. (2018) |
| Cyberbiosecurity "focuses primarily on how cyber assets (for instance, computer networks) can affect biosecurity, which is '... generally associated with travel, supply chains, terrorist activities, and defense,' though it is also of marked importance in academic settings with high amounts of trust." | Potter and Palmer (2023) |
| "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." | Richardson et al. (2019a) |
| "Cyberbiosecurity is a new field that brings together different disciplines in new ways, triggering a pressing need for new thinking in terms of relevant threats, vulnerabilities, and consequences." | Schabacker et al. (2019) |
| "If we examine the term 'cyberbiosecurity' through the lens of interdisciplinary collaboration, the field would represent the act of applying biosecurity best practices to the cyber domain." | Titus et al. (2023) |

While ambiguities may currently exist and the convergence of the disciplines that make up cyberbiosecurity are not explicit, merely applying cyber tools to biology-specific techniques is a simplistic and reductionist view of the field. Richardson et al.'s (2019b) description of a cyberbiosecurity professional provides a notable perspective: "A cyberbiosecurity professional is a practitioner with requisite foundational understanding of biological science principles and practice, fluency in IT lexicon and management, and concept mastery of risk and threat assessment." To adequately work toward safeguarding ALS critical infrastructures, a cyberbiosecurity professional must deploy this knowledge base to understanding the scope and impact of cyberbiosecurity risks across a combination of areas of concern, including general scope and consequences, food, agriculture, and water, biological databases, public health, national and transnational concerns, etc., depending on professional orientations (Mueller, 2021).

Aggregating and aligning different perspectives into a broadened yet precise definition can promote a comprehensive understanding of the key concepts of cyberbiosecurity and flatten ambiguities. Particularly, "defining the key elements of the emerging field of cyberbiosecurity is important to ensuring a common understanding of the relevant technical issues that arise from this new hybrid discipline" (Schabacker et al., 2019). Understanding the pathway to integrative cyberbiosecurity education programming begins here. Definitions need to be synthesized to reflect common, generated frameworks that enhance clarity and promote professional learning opportunities about cyberbiosecurity across relevant stakeholder communities.

## Shadow or Pseudo-Shadow Education: Current State of Cyberbiosecurity

Given the current lack of standardized programs, educational endeavors in cyberbiosecurity may be understood as shadow education (Zhang and Bray, 2020), because most learning opportunities/activities in cyberbiosecurity exist outside formal educational curricula, including conferences, workshops, seminars, or even through access to the limited but growing body of literature. Atypical of conventional shadow education (Stevenson and Baker, 1992; Bray, 2010; Zhang and Bray, 2020), existing (shadow) cyberbiosecurity education does not follow any formal or standardized cyberbiosecurity programs, as there is none to mimic. Current educational efforts are at best a mimicry of different aspects of the fields that comprise the convergence domain of cyberbiosecurity. Given this deviation from what shadow education is typically known to be, we posit the current state of cyberbiosecurity education as pseudo-shadow education. The pseudo-shadow nature of cyberbiosecurity is largely responsible for the nebulousness surrounding the definition.

In an attempt to understand the capability maturity (White, 2021) of cyberbiosecurity education across stakeholders, perspectives from an online survey (Adeoye et al., 2023) confirm the shadowy state of cyberbiosecurity: *"There are a lot of gaps when it comes to actual education as opposed to PowerPoint slides."* Similarly, another related comment reinforced the concern of educational program availability: *"I am not familiar with any cyberbiosecurity courses; I am only familiar with conferences/symposiums that touch on cyberbiosecurity."* Apart from conferences, few educational efforts (case studies, curricula, webinars) with limited but growing visibility are available (e.g., see Ag Decision Maker (n.d.); Miller et al. (2022); Kaufman et al. (2023); Lindberg and Bagby (2023)). This status quo affects the degree to which professionals can be prepared to handle the challenges of the cyberbiosecurity threat landscape.

While we have presented a description of a cyberbiosecurity professional as a cross-disciplinary practitioner, the question remains: how can integrative education programming help prepare this professional to think and act in the presence of emerging threats? This will require conscious investment in rich research and practice that considers building a cyberbiosecurity community comprising relevant interdisciplinary stakeholder groups: academia, research, and industry. Underlying considerations for cyberbiosecurity community building are clear definitions and construction of boundaries about traditional approaches within cybersecurity and biosecurity and identifying relevant entry points, limitations, and intersections toward integrative education

and professional workforce development. Ultimately, integrative cyberbiosecurity education programming will benefit from community relevance and disciplinary and market perspectives (Richardson et al., 2019b).

## Suggestions for Building the Foundation of Cyberbiosecurity Education

Our analyses so far indicate that building an integrative cyberbiosecurity education to facilitate research and practice is an indispensable endeavor. Toward this end, we present suggestions and considerations, highlighting the import of data literacy as an entry requirement into cyberbiosecurity and recommend an expandable cyberbiosecurity education framework.

### *Data Literacy as a Baseline Skill Required for Cyberbiosecurity*

Data science and data literacy play a crucial role in engaging learners and educational programs in cyberbiosecurity. The bioeconomy is vulnerable to cyber threats, and the dependence on proprietary intellectual property, cyber-physical systems, and government-regulated production environments makes it essential to have a strong understanding of data science and cybersecurity (Titus et al., 2023). Yet insufficient effort is geared toward obtaining, tracking, organizing, and analyzing data related to the risks of cyberattacks on ALS systems (Guttieres et al., 2019). This may be due to a lack of sufficient knowledge in data science and literacy or inadequate understanding of the relevance of data science skills in promoting threat/risk identification, prevention, and mitigation, or a combination of all. Data literacy is a fundamental skill necessary for understanding and analyzing data. It is essential to incorporate statistical literacy augmented by data literacy into the early stages of the professional development of the workforce dealing with cyberbiosecurity concerns. The interdisciplinary nature of cyberbiosecurity requires communication and collaboration within the multisector system to address issues related to the privacy of data producers, ownership of original data, risks of data sharing, security protection for data transfer and storage, and public perceptions of the food supply chain (Duncan et al., 2020).

The emerging discipline of cyberbiosecurity seeks to safeguard the bioeconomy by analyzing the system and identifying priorities to develop a campaign and timeline. The possibility of applying existing computer literacy education to data science education has been examined, and it has been found that it is possible to use the report assignments in the lectures and the results of questionnaires to teach data science (Farrell and Robertson, 2019). We suggest that interacting with biology and agriculture professionals via the routes of data literacy and data science as initial encounter topics can ease the imposter burden associated with cyberbiosecurity. This approach can help learners understand the importance of data science and cybersecurity in the bioeconomy and how it relates to their disciplinary field. Data science can be a starter route for the professional development of the biological and agricultural workforce, as it can help them develop skills in high demand in the job market.

### *Cyberbiosecurity Education Framework (CEF)*

We present a Cyberbiosecurity Education Framework (CEF) for mapping the landscape of and communicating cyberbiosecurity to practitioners, including farmers, producers, supply chain experts, and operators of ag-related systems such as irrigation, water distribution systems, and smart farms. The CEF follows a set of systematic activities grounded in the DMAIC (Define, Measure, Analyze, Improve, and Control) process and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (American Society for Quality, n.d.; NIST, 2018; Batarseh et al., 2021; Freeman et al., 2021). CEF is built on the foundation of the underlying issues of interdisciplinarity, threat landscape, community building, nebulous definition, and data and digital literacy to support integrative cyberbiosecurity education programming for workforce development. The combination of the traditional data-driven DMAIC process and the NIST framework is to bridge the gap and create a balance between data- and user-focused processes, which are both required in cyberbiosecurity education programming.

The CEF consists of five non-exhaustive and expandable phases, namely: Identify and Define Cyberbiosecurity Threats; Measure Data and Data Tools; Characterize Cyber and Human Contexts; Plan Cyberbiosecurity Strategy; and, Execute, Monitor, and Improve (fig. 4). Phase One of the CEF seeks to identify and define the problem at hand in line with the prevailing cyberbiosecurity threat landscape. The confluence of different disciplines and challenges makes this phase critical for professionals interfacing with the convergence domain of cyberbiosecurity. Although the NIST framework has no particular implementation order (Krumay et al., 2018), the CEF leans toward the DMAIC process in this regard and prioritizes Phase One (Identification and Definition) as a starting point for cyberbiosecurity education/training. This prioritization is also consistent with the NIST assertion that "the activities in the Identify Function are foundational for effective use of the Framework" (National Institute of Standards and Technology, 2018).


**Figure 4. The Cyberbiosecurity Education Framework (CEF).**

Phase Two, the Measure phase, identifies means to assess the security of the biological and cyber components in the cyberbiosecurity environment or organization. This involves identification, understanding, and measuring sensors or tools that collect data (for instance, how many data points per day, what network security protocols are applied, and so on), and those used to govern certain procedures (such as on-premise computational systems). We advocate both quantitative and qualitative data interaction at this stage, as some situations are not easily quantifiable. Cyber threat intelligence and risk management rely on both qualitative and quantitative data analysis for making accurate decisions in protecting IT and OT systems. Data is the food for threat intelligence, just like "threat intelligence is like food for malnourished risk models" (Baker, 2016). Lacking any relevant data type in the intelligence process can lead to a deficient understanding of the cyberbiosecurity threat landscape.

Phase Three, Characterize Cyber and Human Contexts, captures the multidimensional set of constructs that includes the operational environment, economic factors, weather events, and other factors affecting the security of the agro-biological systems and infrastructures. Beyond capturing the inherent data, translating this data into meaningful, insightful, and usable forms that consider the computer-human interaction for optimal decision-making is an important task that cyberbiosecurity professionals should learn. In this phase (three), cyberbiosecurity professionals would learn the science of teaming and information-sharing to leverage on cross-disciplinary strengths and opportunities.

In Phase Four, planning a cyberbiosecurity strategy must also consider the multidimensionality of cyberbiosecurity, and especially bridge potential gaps between data-driven and user-driven processes and human and computer interactions. This strategy stage transcends merely putting policies in place, but looks at different pros and cons of existing or new policies and addresses strategic means to translate policies into actionable processes. Cyberbiosecurity professionals need to learn how to harness the multi-dimensionalities comprising their convergence domain by analyzing and synthesizing them into adaptable strategies that help to build formidable protection and resilience around their operational environments. Investing in and building security infrastructures does not eliminate threats or guarantee the absence of attacks or intrusions; cyberbiosecurity strategy must accommodate plans for prevention and recovery.

In Phase Five, professionals should learn the process of executing, monitoring, and improving cyberbiosecurity strategies. Taking action may be easier said than done, especially when it involves complex systems and situations, but a well-thought-out strategic plan will help to ease the challenges. Actions must be calculated and relevant to the cyberbiosecurity environment. Because of the continuous advances in technology and constant changes in security requirements, both technical and non-technical, actions must be observed and relevant data collected to monitor and evaluate progress and current usefulness. Relevant changes to improve the protection, response, and resilience of the cyberbiosecurity environment must be constantly pursued. The execution of cyberbiosecurity strategies should be backed with continuous measured improvement.

Premising cyberbiosecurity education and training on the CEF offers opportunities for integrative education programming. While we suggest a step-wise, systematic approach to using the CEF, the framework relies on an iterative process to accommodate and explore different dimensions of cyberbiosecurity. When implementing this framework, cyberbiosecurity professionals need to consider the complex and fluid nature of their domain and must be trained to revisit previous steps as many times as required to unravel new findings as more information about the threat landscape becomes available. Educators must emphasize the need for and importance of iteration when designing cyberbiosecurity education programs using the CEF. The CEF offers potential for gathering data and understanding human interactions with the dynamic cyberbiosecurity environment to build robust education programming.

## CONCLUSIONS

Cyberbiosecurity is an emerging field at the convergence of digital technology and agriculture and life sciences (ALS). This convergence occasions emerging, unconventional challenges in critical infrastructure security related to ALS. Because the ALS industry is unfamiliar with cyber challenges, it is difficult for professionals operating within the cyberbiosecurity domain to navigate the emerging challenges and adequately safeguard the bioeconomy against unwanted and unwarranted intrusions. The limited understanding of the biological environment also makes the digital security professional solely unsuited for the new challenges. Understanding the convergence of both worlds – digital technology and ALS – and the accompanying new threat landscape is the primary basis of cyberbiosecurity. However, frameworks for integrative education and training to support the skills development of people working in cyberbiosecurity-related industries are lacking. Concerns impacting an integrative process in cyberbiosecurity include alignment in definition, interdisciplinary community building, the peculiar dynamics of the cyberbiosecurity threat landscape, and data and digital literacy skills.

Integrative cyberbiosecurity education programming seeks to produce cyberbiosecurity professionals. A cyberbiosecurity professional is a practitioner with relevant foundational understanding of biological processes and practice, IT skills and management, and mastery of cyberbiosecurity risk and threat landscape, coupled with the ability to identify, define, and assess risks and threats and deploy requisite security strategies while working in an interdisciplinary environment. Developing a cyberbiosecurity professional is challenging. We propose a Cyberbiosecurity Education Framework (CEF) that provides a systematic and iterative protocol for training workers in the convergence domain of cyberbiosecurity. The CEF has five non-exhaustive and expandable phases designed to equip cyberbiosecurity educators and professionals to navigate the arduous process of cyberbiosecurity knowledge creation and transfer and skills development. The systematic and iterative phases are Identify and Define Cyberbiosecurity Threat, Measure Data and Data Tools, Characterize Cyber and Human Contexts, Plan

Cyberbiosecurity Strategy, and Execute, Monitor, and Improve. As a framework that relies on data, human experience, and the ever-changing technological environment for improvement and expansion, the CEF offers opportunities of future studies for researchers, educators, and practitioners to test and apply the framework to mapping the landscape of and educating the workforce in the related domains of cyberbiosecurity.


### ACKNOWLEDGMENTS

The authors acknowledge the Virginia Tech University Libraries Collaborative Research Grant Program for supporting this study. This work was supported [in part] by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit www.cyberinitiative.org.


## REFERENCES


Adeoye, S., Kaufman, E. K., Brown, A. M., & Batarseh, F. A. (2023). Mapping the landscape of cyberbiosecurity education. *Proc. Commonwealth Cyber Initiative - CCI Symp.* VTechWorks. Retrieved from http://hdl.handle.net/10919/114739

Ag Decision Maker, Iowa State University. (n.d.). Improving cybersecurity information: Cybersecurity for Iowa farmers and rural businesses. Retrieved from https://www.extension.iastate.edu/agdm/info/cybersecurity.html

Ahmadpour, A., & Mirdamadi, M. (2010). Determining challenges in the application of e-learning in agricultural extension services in Iran. *Am. Eurasian J. Agric. Environ. Sci., 9*(3), 292-296.

American Society for Quality. (n.d.). The define measure analyze improve control (DMAIC) process. Retrieved from https://asq.org/quality-resources/dmaic#

Arntz, P. (2021). FBI warns of ransomware threat to food and agriculture. Malwarebytes. Retrieved from https://www.malwarebytes.com/blog/news/2021/09/fbi-warns-of-ransomware-threat-to-food-and-agriculture

Baker, L. M., Boyer, C. R., & Boyer, R. (2022). Selling safely: Cybersecurity best practices for small, rural Ag businesses: WC416/AEC755, 5/2022. *EDIS, 2022*(3). https://doi.org/10.32473/edis-wc416-2022

Baker, W. (2016). Introduction to threat intelligence and risk management. FAIR Institute. Retrieved from https://www.fairinstitute.org/blog/introduction-to-threat-intelligence-and-risk-management

Batarseh, F. A., & Kulkarni, A. (2023). AI for water. *Computer, 56*(3), 109-113. https://doi.org/10.1109/MC.2022.3231142

Batarseh, F. A., Freeman, L., & Huang, C.-H. (2021). A survey on artificial intelligence assurance. *J. Big Data, 8*(1), 60. https://doi.org/10.1186/s40537-021-00445-7

Bauman, S., Underwood, M. K., & Card, N. A. (2013). Definitions: Another perspective and a proposal for beginning with cyberaggression. In S. Bauman, D. Cross, & J. Walker (Eds.), *Principles of cyberbullying research: Definition, methods, and measure* (pp. 41-45). Routledge. https://doi.org/10.4324/9780203084601

Berger, K. M., & Schneck, P. A. (2019). National and transnational security implications of asymmetric access to and use of biological data. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00021

Blair, B. (2012). Elastic minds? Is the interdisciplinary/multidisciplinary curriculum equipping our students for the future: A case study. *Art Des. Commun. High. Educ., 10*(1), 33-50. https://doi.org/10.1386/adch.10.1.33_1

Bray, M. (2010). Researching shadow education: Methodological challenges and directions. *Asia Pac. Educ. Rev., 11*(1), 3-13. https://doi.org/10.1007/s12564-009-9056-6

Briguglio, L., & Moncada, S. (2019). The benefits and downsides of multidisciplinary education relating to climate change. In W. L. Filho, & S. L. Hemstock (Eds.), *Climate change and the role of education* (pp. 169-187). Cham: Springer. https://doi.org/10.1007/978-3-030-32898-6_10

Brumfield, C. (2022). News analysis: Remote bricking of Ukrainian tractors raises agriculture security concerns. CSO. Retrieved from https://www.csoonline.com/article/3661434/remote-bricking-of-ukrainian-tractors-raises-agriculture-security-concerns.html

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The diamond model of intrusion analysis [Technical Report]. Hanover, MD: Center for Cyber Intelligence Analysis and Threat Research. Retrieved from http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Cheein, F. A., & Carelli, R. (2013). Agricultural robotics: Unmanned robotic service units in agricultural tasks. *IEEE Ind. Electron. Mag., 7*(3), 48-58. https://doi.org/10.1109/MIE.2013.2252957

Chi, H., Welch, S., Vasserman, E., & Kalaimannan, E. (2017.). A framework of cybersecurity approaches in precision agriculture. In A. R. Bryant, J. R. Lopez, & R. F. Mills (Ed.), *Proc. 12th Int. Conf. on Cyber Warfare and Security*, (pp. 90-95).

Choi, B. C., & Pak, A. W. (2006). Multidisciplinarity, interdisciplinarity and transdisciplinarity in health research, services, education and policy: 1. Definitions, objectives, and evidence of effectiveness. *Clin. Investig. Med., 29*(6), 351-364.

Cooper, C. (2015). Cybersecurity in food and agriculture. In J. LeClair (Ed.), *Protecting our future* (Vol. 2). Hudson Whitman.

Creasey, S. (2023). Tech leaves food industry more exposed to cybersecurity threat. JustFood. Retrieved from https://www.just-food.com/features/tech-leaves-food-industry-more-exposed-to-cybersecurity-threat/

Cybersecurity and Infrastructure Security Agency. (2021). Cybersecurity advisory: Ongoing cyber threats to U.S. water and wastewater systems. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

Cybersecurity Infrastructure Security Agency. (n.d.). Advanced persistent threats. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats#

DiEuliis, D. (2023). Revisiting the digital biosecurity landscape. In D. Greenbaum (Ed.), *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 71-78). Cham: Springer. https://doi.org/10.1007/978-3-031-26034-6_5

Drape, T. A., & Murch, R. (2022). Leveraging cyberbiosecurity to safeguard agriculture and food. Virginia Tech. Retrieved from http://hdl.handle.net/10919/112168

Drape, T., Magerkorth, N., Sen, A., Simpson, J., Seibel, M., Murch, R. S., & Duncan, S. E. (2021). Assessing the role of cyberbiosecurity in agriculture: A case study. *Front. Bioeng. Biotechnol., 9*. https://doi.org/10.3389/fbioe.2021.737927

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K.,... Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00063

Duncan, S. E., Zhang, B., Thomason, W., Ellis, M., Meng, N., Stamper, M.,... Drape, T. (2020). Securing data in life sciences — A plant food (edamame) systems case study. *Front. Sustain., 1*. https://doi.org/10.3389/frsus.2020.600394

Elhassan, I. B. (2012). Multidisciplinary curriculum to teaching english language in Sudanese institutions (a case study). *Theor. Pract. Lang. Stud., 2*(2), 402-406. https://doi.org/10.4304/tpls.2.2.402-406

Farrell, K., & Robertson, J. (2019). Interdisciplinary data education: Teaching primary and secondary learners how to be data citizens. *Proc. 14th Workshop in Primary and Secondary Computing Education: WiPSCE '19.* Association for Computing Machinery. https://doi.org/10.1145/3361721.3362120

FBI & USDA, FDA OCI. (2022). Criminal actors use business email compromise to steal large shipments of food products and ingredients. Joint Cybersecurity Advisory AA22-340A. Retrieved from https://www.ic3.gov/Media/News/2022/221216.pdf

FBI. (2021). Cyber criminal actors targeting the food and agriculture sector with ransomware attacks. Private Industry Notification, 20210901-001. Retrieved from https://www.ic3.gov/Media/News/2021/210907.pdf

FBI. (2022). Ransomware attacks on agricultural cooperatives potentially timed to critical seasons. Private Industry Notification, 20220420-001. Retrieved from https://www.ic3.gov/Media/News/2022/220420-2.pdf

Freeman, L., Rahman, A., & Batarseh, F. A. (2021). Enabling artificial intelligence adoption through assurance. *Soc. Sci., 10*(9), 322. https://doi.org/10.3390/socsci10090322

Freeth, R., & Caniglia, G. (2020). Learning to collaborate while collaborating: Advancing interdisciplinary sustainability research. *Sustain. Sci., 15*(1), 247-261. https://doi.org/10.1007/s11625-019-00701-z

Glebe, R. (2020). Why pursue a degree program with a multidisciplinary approach? GoAbroad. Retrieved from https://www.goabroad.com/articles/degree-abroad/advantages-of-multidisciplinary-curriculum

Greenbaum, D. (2023). *Cyberbiosecurity: A new field to deal with emerging threats.* Cham: Springer Nature. https://doi.org/10.1007/978-3-031-26034-6

Guttieres, D., Stewart, S., Wolfrum, J., & Springs, S. L. (2019). Cyberbiosecurity in advanced manufacturing models. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00210

Jones, D. (2023). Dole incurs $10.5M in direct costs from February ransomware attack. Cybersecurity Dive. Retrieved from https://www.cybersecuritydive.com/news/dole-10m-costs-ransomware/650711/

Jung, J., Maeda, M., Chang, A., Bhandari, M., Ashapure, A., & Landivar-Bowles, J. (2021). The potential of remote sensing and artificial intelligence as tools to improve the resilience of agriculture production systems. *Curr. Opin. Biotechnol., 70*, 15-22. https://doi.org/10.1016/j.copbio.2020.09.003

Kaufman, E., Adeoye, S., & Batarseh, F. (2023). Leadership for CyberBioSecurity: The case of Oldsmar Water. VTechWorks. Retrieved from http://hdl.handle.net/10919/113624

Kovacs, E. (2021). Asian food distribution giant JFC International hit by ransomware. SecurityWeek. Retrieved from https://www.securityweek.com/asian-food-distribution-giant-jfc-international-hit-ransomware/

Krumay, B., Bernroider, E. W. N., & Walser, R. (2018). Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework. In N. Gruschka (Ed.), Secure IT systems (pp. 369–384). Springer. https://doi.org/10.1007/978-3-030-03638-6_23

Kulkarni, A., Yardimci, M., Sikder, M. N., & Batarseh, F. A. (2023). P2O: AI-driven framework for managing and securing wastewater treatment plants. *J. Environ. Eng., 149*(9), 04023045. https://doi.org/10.1061/JOEEDU.EEENG-7266

Lindberg, H., & Bagby, B. (2023). CyberBioSecurity training module for life science. Retrieved from https://osf.io/63agh/wiki/home/?view_only=8a829e39cf474b62a0f4336880ca8f5d

Mantle, J. L., Rammohan, J., Romantseva, E. F., Welch, J. T., Kauffman, L. R., McCarthy, J.,… Lee, K. H. (2019). Cyberbiosecurity for biopharmaceutical products. *Front. Bioeng. Biotechnol.*, *7*, 116. https://doi.org/10.3389/fbioe.2019.00116

Miller, R. J., Yun, Y., Ray, A., & Duncan, S. E. (2022). Securing the food industry: An introduction to cyberbiosecurity for food science. VTechWorks. Retrieved from http://hdl.handle.net/10919/111375

Monteiro, J., & Barata, J. (2021). Artificial intelligence in extended agri-food supply chain: A short review based on bibliometric analysis. *Procedia Comput. Sci., 192*, 3020-3029. https://doi.org/10.1016/j.procs.2021.09.074

Mueller, S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? *Biosaf. Health, 3*(1), 11-21. https://doi.org/10.1016/j.bsheal.2020.09.007

Murch, R. (2023). Introduction: Origin and intent for the new field of cyberbiosecurity. In D. Greenbaum (Ed.), *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 7-15). Cham: Springer. https://doi.org/10.1007/978-3-031-26034-6_2

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

Murch, R., & DiEuliis, D. (2019). Editorial: Mapping the cyberbiosecurity enterprise. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00235

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

National Sanitation Foundation. (2022). A single attack disrupted beef prices and prompted calls for improved security. Retrieved from https://www.nsf.org/blog/consumer/cybersecurity-food-agriculture

Nikander, J., Manninen, O., & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Comput. Electron. Agric., 179*, 105776. https://doi.org/10.1016/j.compag.2020.105776

Potter, L., & Palmer, X.-L. (2023). Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In D. Greenbaum (Ed.), *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 37-69). Cham: Springer. https://doi.org/10.1007/978-3-031-26034-6_4

Ramirez-Asis, E., Vilchez-Carcamo, J., Thakar, C. M., Phasinam, K., Kassanuk, T., & Naved, M. (2022). A review on role of artificial intelligence in food processing and manufacturing industry. *Mater. Today: Proc., 51*(8), 2462-2465. https://doi.org/10.1016/j.matpr.2021.11.616

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019a). Cyberbiosecurity: A call for cooperation in a new threat landscape. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00099

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019b). Building capacity for cyberbiosecurity training. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00112

Rodríguez, E., Otero, B., Gutiérrez, N., & Canal, R. (2021). A survey of deep learning techniques for cybersecurity in mobile networks. *IEEE Commun. Surv. Tutor., 23*(3), 1920-1955. https://doi.org/10.1109/COMST.2021.3086296

Russell, C. (2022). Cyber security in digital agriculture: Investigating farmer perceptions, preferences, & expert

knowledge. MS thesis. Canada: University of Guelph. Retrieved from https://hdl.handle.net/10214/27219

Salam, A. (2020). Internet of things for sustainability: Perspectives in privacy, cybersecurity, and future trends. In *Internet of things for sustainable community development: Wireless communications, sensing, and systems* (pp. 299-327). Cham: Springer. https://doi.org/10.1007/978-3-030-35291-2_10

Schabacker, D. S., Levy, L.-A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Front. Bioeng. Biotechnol., 7*. https://doi.org/10.3389/fbioe.2019.00061

Schreurs, H. (2015). Creating a multidisciplinary curriculum in practice oriented education and research. *European J. Soc. Educ., 26/27*, 91-102.

Schroeder, K., Lampietti, J., & Elabed, G. (2021). *What's cooking: Digital transformation of the agrifood system.* World Bank Group. https://doi.org/10.1596/978-1-4648-1657-4

Sikder, M. N., Nguyen, M. B., Elliott, E. D., & Batarseh, F. A. (2023). Deep H2O: Cyber attacks detection in water distribution systems using deep learning. *J. Water Process Eng., 52*, 103568. https://doi.org/10.1016/j.jwpe.2023.103568

Sobien, D., Yardimci, M. O., Nguyen, M. B., Mao, W.-Y., Fordham, V., Rahman, A.,... Batarseh, F. A. (2023). Ai for cyberbiosecurity in water systems — a survey. In D. Greenbaum (Ed.), *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 217-263). Cham: Springer. https://doi.org/10.1007/978-3-031-26034-6_13

Sontowski, S., Gupta, M., Chukkapalli, S. S., Abdelsalam, M., Mittal, S., Joshi, A., & Sandhu, R. (2020). Cyber attacks on smart farming infrastructure. *Proc. 2020 IEEE 6th Int. Conf. on Collaboration and Internet Computing (CIC)* (pp. 135-143). IEEE. https://doi.org/10.1109/CIC50333.2020.00025

Spaulding, A., & Wolf, J. R. (2018). Cyber-security knowledge and training needs of beginning farmers in Illinois. *Proc. 2018 Agricultural & Applied Economics Association Annual Meeting.*

Stephen, S., Alexander, K., Potter, L., & Palmer, X. L. (2023). Implications of cyberbiosecurity in advanced agriculture. *Proc. 18th Int. Conf. on Cyber Warfare and Security*, (pp. 387-393). https://doi.org/10.34190/iccws.18.1.995

Stevenson, D. L., & Baker, D. P. (1992). Shadow education and allocation in formal schooling: Transition to university in Japan. *Am. J. Sociol., 97*(6), 1639-1657. https://doi.org/10.1086/229942

Titus, A. J., Hamilton, K. E., & Holko, M. (2023). Cyber and information security in the bioeconomy. In D. Greenbaum (Ed.), *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 17-36). Cham: Springer. https://doi.org/10.1007/978-3-031-26034-6_3

USDA-NASS. (2021). Farm computer usage and ownership. Retrieved from https://usda.library.cornell.edu/concern/publications/h128nd689

White, S. R. (2021). What is CMMI? A model for optimizing development processes. CIO. https://www.cio.com/article/274530/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html

Yaman, R., Vardai, N., & Yaman, G. (2005). Sandwich programs for multidisciplinary engineering education. *Proc. 2005 6th Int. Conf. on Information Technology Based Higher Education and Training*, (pp. T4A/18-T4A/22). https://doi.org/10.1109/ITHET.2005.1560254

Zhang, W., & Bray, M. (2020). Comparative research on shadow education: Achievements, challenges, and the agenda ahead. *Eur. J. Educ., 55*(3), 322-341. https://doi.org/10.1111/ejed.12413