Cyberbiosecurity Workforce Preparation: Education at the Convergence of Cybersecurity and Biosecurity

Samson O. Adeoye[1], Heather Lindberg[2], B. Bagby[3], Anne M. Brown[4], Feras A. Batarseh[5], and Eric K. Kaufman[1]

[1]Department of Agricultural, Leadership, and Community Education, Virginia Tech
[2]Department of Biology, Virginia Western Community College
[3]Center for Cybersecurity, Virginia Western Community College
[4]Research and Informatics, University Libraries, Virginia Tech
[5]Department of Biological Systems Engineering, Virginia Tech

Samson O. Adeoye https://orcid.org/0000-0001-9920-1539
Anne M. Brown https://orcid.org/0000-0001-6951-8228
Feras A. Batarseh https://orcid.org/0000-0002-6062-2747
Eric K. Kaufman https://orcid.org/0000-0001-8009-0066

The authors have no conflict of interest to declare. This work was funded by the Workforce Development Program of the Commonwealth Cyber Initiative Southwest Virginia (CCI SWVA) node.

Correspondence concerning this article should be addressed to Eric K. Kaufman, Virginia Tech Department of Agricultural, Leadership, and Community Education, 214 Litton-Reaves Hall (MC 0343), 175 West Campus Dr, Blacksburg VA 24061.
Email: ekaufman@vt.edu

Abstract

Cyberbiosecurity is an emerging field at the convergence of life sciences and the digital world. As technological advances improve operational processes and expose them to vulnerabilities in agriculture and life sciences, cyberbiosecurity has become increasingly important for addressing contemporary concerns. Unfortunately, at this time, educational opportunities for cyberbiosecurity workforce preparation are limited. Stakeholders' perceptions may help guide cyberbiosecurity workforce preparation efforts and bridge the gap from the classroom to the field. Toward this end, we identified stakeholders in education, private industry, and state agencies in Virginia and sought their input through both an online survey and focus groups. Findings suggest limited awareness and understanding of cyberbiosecurity. Results indicate that both formal and non-formal learning components—including short modules and comprehensive standalone courses—are important for cyberbiosecurity education programming. Stakeholders tied potential success of education programming to systems thinking and collaborative designs. Moreover,

results reveal insights into concerns at the convergence of information technology (IT) and operational technology (OT), which is central to effective workforce preparation for today's agriculture and life sciences professionals. Continuous interdisciplinary collaboration and academia-industry partnerships will be critical for developing robust cyberbiosecurity education and securing the future of agriculture.

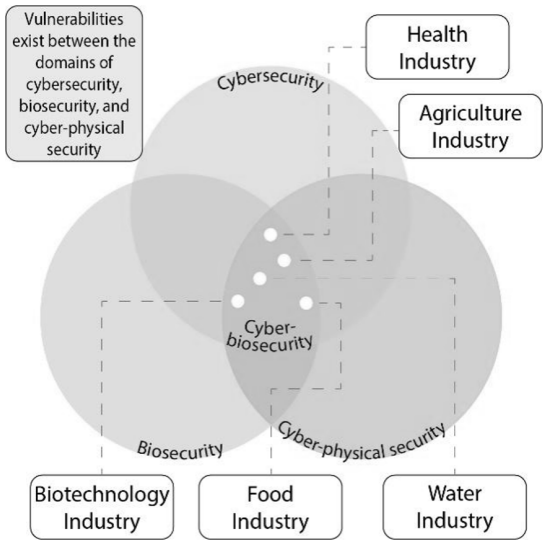
Keywords: cyberbiosecurity, education programming, workforce development, stakeholders, collaboration

While the agricultural industry has historically been viewed as disconnected from the cyber world (Bryne, 2019), the Federal Bureau of Investigation (FBI) is increasingly concerned about cyber-criminal actors targeting the food and agriculture sector (FBI, 2016; 2021; 2022; FBI et al., 2022). Indeed, as technological advances have improved operational processes in agriculture, the workforce increasingly interacts with cyber-physical systems and the Internet of Things (IoTs) (Chi et al., 2017; Drape & Murch, 2022; Freyhof et al., 2022; Jung et al., 2021; Monteiro & Borata, 2021; Ramirez-Asis et al., 2022; Subeesh & Mehta, 2021). The life sciences' conventional approaches to biosafety and biosecurity are insufficient for protecting against emerging cyber risks (Berger & Schneck, 2019; Duncan et al., 2019; Sobien et al., 2023). Moreover, conventional approaches to cybersecurity are insufficient for protecting against emergent threats to human health and biological life (Murch et al., 2018; Pauwels, 2021; Titus et al., 2023; Walsh, 2022). As noted by AI EdgeLabs (2022), "High-impact and sophisticated assaults on vital infrastructure organizations, including agriculture, are becoming increasingly widespread around the world, posing a serious threat to the food chain, human, and livestock food security" (para. 22). Although educational programming is a reliable strategy for addressing such concerns, effective programming relies on research that conveys the practical reality of various stakeholders (Crawford & Fink, 2019; Degreenia & Sutton, 2020; Watson et al., 2019). The gap between education and current realities is where lies the challenge with improving the "education-to-workforce pipeline," and conscious attempts must be made to mend the broken links by making education capable of addressing societal concerns (Adeoye & Kaufman, 2023).

Through years of research and industry engagements, the priority for cyberbiosecurity has emerged from a realization that separate approaches to biosecurity and cybersecurity are insufficient (Drape et al., 2021; Greenbaum, 2023; Murch, 2023). As an emerging field at the interface of the life sciences and the digital world, cyberbiosecurity intersects several domains of interest for colleges and teachers of agriculture (Figure 1; Duncan et al., 2019). The "bio" emphasis is central to the Cyber+Bio+Security field. At the heart of the "bio" component are agriculture and life science graduates who often work in industrial sectors that control water, food processing, etc. In order to maintain the integrity, accessibility and security of biological data, these graduates must be prepared to interface with information technologists, computer scientists, or software engineers who are unfamiliar with the unique aspects of the life sciences (Mueller, 2021; Richardson, Conell, et al., 2019).

Figure 1.

Overlapping Functions and Domains of Cyberbiosecurity



Note. Adapted from "Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system," by S. E. Duncan et al., 2019, Frontiers in Bioengineering and Biotechnology, 7, 63, p. 2 (https://doi.org/10.3389/fbioe.2019.00063).

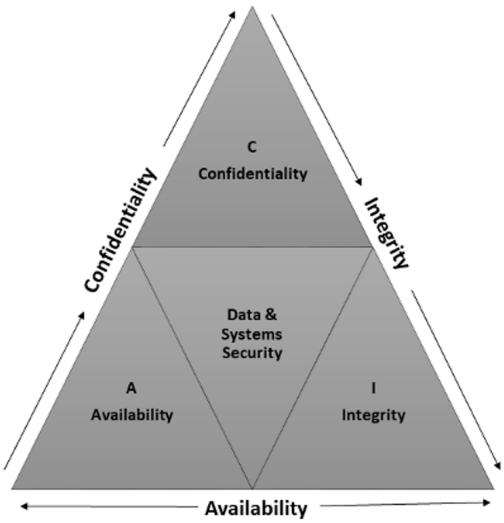
Given the growing body of knowledge in the field and the continuous automation of agricultural and biological systems, the relevance of cyberbiosecurity is unquestionable (Sinha & Dhanalakshmi, 2022; Sobien et al., 2023; Stephen et al., 2023). However, educational opportunities to prepare professionals for the future of work in cyberbiosecurity remain scarce (Adeoye et al., 2023; Richardson, Lewis, et al., 2019). While there appears to be consensus in terms of its relevance among educators, researchers, and industry experts, little is known about programmatic efforts in cyberbiosecurity in higher education (Drape et al., 2021). This potentially reinforces a breach in the education-to-workforce pipeline and complicates the concerns of the "skills gap and whether a graduate will be fit for the contemporary workforce" (Kaufman & Adeoye, 2023, p. 1). To maintain or create a strong cyberbiosecurity pipeline, it is necessary to cross-train agriculture, biology, environmental, food science, or related domain experts in cyberbiosecurity fundamentals (Duncan et al., 2021). By preparing individuals outside of the common scope of cybersecurity, it is suggested that we will have a more prepared and proactive workforce, ready for threats to agriculture, life sciences, and the related critical infrastructures (Richardson, Conell, et al., 2019).

The priorities for cybersecurity can be usefully framed in terms of confidentiality, integrity, and availability – the CIA triad (Figure 2). Researchers believe the CIA triad constitutes an important model for understanding information security and provides a basis upon which systems protection and systems and organization resilience are built (Nikander et al., 2020; van der Ham, 2021). Confidentiality focuses on privacy of personal or critical data, fostering trust for individuals

and organizations. Integrity emphasizes the accuracy and reliability of data, protecting it from unauthorized alteration or compromise. Availability implies uninterrupted access and functionality of systems for authorized operators or users at all times. A cybersecurity concern is imminent where any of the components of the triad is breached, resulting in loss of confidentiality, unauthorized data or systems alteration, and/or loss of access to systems by authorized personnel or system dysfunctionality (Yeboah-Boateng, 2013).

Figure 2.

The Confidentiality, Integrity, Availability (CIA) Triad



Note. In the public domain.

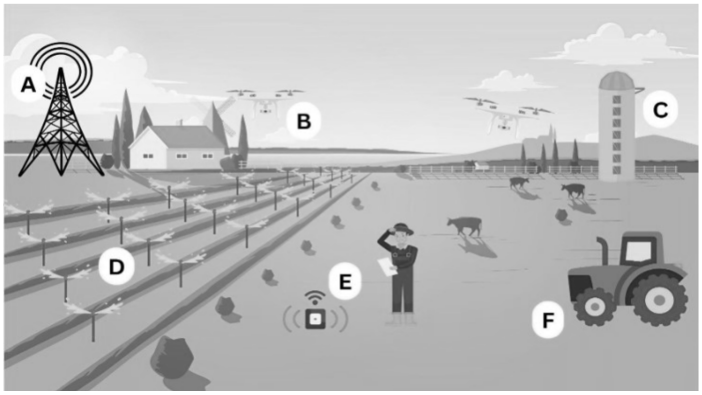
Like cybersecurity, biosecurity has many interpretations. Waage and Mumford (2008) summarized biosecurity as the protection against pests and diseases and biological weapons, the actions taken to mitigate the risk of the spread of possible attacks and diseases, including zoonotic and reverse zoonotic diseases, and the policies and regulations involved. To ensure adequate protection, biosecurity measures need to be carefully implemented to control infectious diseases, with implementation procedures documented to offer baseline data for monitoring purposes and continuous establishment of relevant sociodemographic characteristics and training requirements (Sayers et al., 2013). Both cybersecurity and biosecurity focus on protection against practices that exploit vulnerabilities that expose critical infrastructures to unwanted and unwarranted attacks. Despite similar focuses, addressing emerging challenges at the intersections of these fields is currently difficult, as each field has different domain knowledge and focuses on different aspects of the emerging threats. The Colorado State University (n.d.) put this difference succinctly: "Traditionally, biosecurity focuses on reducing risks associated with the misuse of life science tools and/or knowledge, whereas cybersecurity is focused on securing information in technology-based systems" (para. 2).

The convergence of cybersecurity and biosecurity appears necessary due to their shared goals, despite the distinct domains they have conventionally maintained. However, the increasing reliance of biosecurity on information technology is not sufficiently considered in planning and implementation strategies toward securing biological systems, highlighting the need for considering the impact of cybersecurity on biosecurity (MacIntyre et al., 2018). Cyberbiosecurity seeks to address "the potential for or actual malicious destruction, misuse, or exploitation of valuable information, processes, and material at the interface of the life sciences and digital worlds" (Richardson, Connell, et al., 2019, p. 2) through contextual mastery and understanding of concepts in the interface of cybersecurity and biosecurity.

The cyberbiosecurity threat landscape is diverse, and concerns can arise at different points in cyber-physical systems (DiEuliis, 2023). The threat landscape is usually not just about traditional data and information security concerns but includes biologically domain-specific knowledge for developing inclusive protection and resilience in the face of emerging challenges. A breach of the CIA in an agricultural environment, for example, may prevent access to critical control systems for ventilation or feeding animals in a dairy farm or poultry or cause alterations in the functioning of electricity or water supply systems, with huge danger of loss of livestock, crops, or environmental damage (Cooper, 2015). Stephen et al. (2023) illustrate the connection between cybersecurity and modern agriculture by identifying possible points of vulnerabilities that cyber attackers can target to exploit the food and agriculture system (Figure 3).

Figure 3.

Example of Cyberbiosecurity Threat Landscape



Note. . Identified attack points include: (A) electrical power grids; (B) drones used on farms; (C) sensors and climate controls of storage silos; (D) water distribution/irrigation systems; (E) agricultural sensors tracking sunlight, humidity, climate, soil air penetration, etc.; and (F) technology used as tools or equipment on farms. From "Implications of cyberbiosecurity in advanced agriculture," by S. Stephen et al., 2023, Proceedings of the 18th International Conference on Cyber Warfare and Security, p. 388 (https://papers.academic-conferences.org/index.php/iccws/article/view/995/977). Reprinted with permission.

Purpose of the Study

The current study was designed to expand upon Richardson, Lewis, et al.'s (2019) efforts with the overarching objective of identifying opportunities for specialized career development and mechanisms for integrated cyberbiosecurity training. Specifically, we sought to synthesize and analyze stakeholders' perceptions

that may guide curricular planning for cyberbiosecurity education. Because cyberbiosecurity is an emerging field of study, the signature pedagogies of the profession are not yet established. Signature pedagogies are "the forms of instruction that leap to mind when we think about the preparation of members of a particular profession" (Shulman, 2005, p. 52). They represent a body of teaching and learning practices that govern the fundamental approach to educating future practitioners in their new professions – in this case cyberbiosecurity – and helping them to develop habits of the mind, heart, and hand (Beck & Eno, 2012; Shulman, 2005; Wayne et al., 2010). Signature pedagogies are important constructs, including knowledge, values, judgments, and ways of thinking, which serve as windows into the underlying cultures of a disciplinary field (Calder, 2006; Shulman, 2005) helping students to "do, think, and value what practitioners in the field are doing, thinking, and valuing" (Calder, 2006, p. 1361).

> Medical schools train physicians through the bedside ritual of clinical rounds; engineering faculty put students together in collaborative-design studios; theological seminaries mingle study with prayer and community service. It is a hallmark of professional education that each discipline has developed characteristic forms of teaching and learning that, like the name of a person written in his own hand, are done in the same way from teacher to teacher and institution to institution. (Calder, 2006, p. 1360)

Being an emerging field with limited educational resources that show current practices, this study anchored on what professionals at the intersection of cybersecurity and biosecurity "do, think, and value." In line with the work of signature pedagogies for the professions, this study attempts to temporally "frame and prefigure the cultures of professional work and provide the early socialization into the practices and values of" cyberbiosecurity (Shulman, 2005, p. 55). While the long-term goal is to establish a sequenced, balanced, and adaptable educational programming, understanding the overall process starts with understanding professionals' perspectives and framing those into signature pedagogical efforts.

Methods

Practitioners in cybersecurity, biosecurity, and related subject areas across Virginia represent the population for this study. This included academic, industry, and government stakeholders who have previously been affiliated with projects related to cybersecurity, biosecurity, and the relevant intersections. The study participants were selected based on their affiliation with and potential knowledge of educational programming for interfacing with the discrete field of cyberbiosecurity. Participants were identified through professional contacts and referrals (snowballing). This convenience sampling is fitting for research in an emerging field like cyberbiosecurity (Emerson, 2021; Jager et al., 2017). The study applied a sequential explanatory mixed method design (quan → QUAL), conducted with a development rationale and a qualitative priority (Creamer, 2017; Guest, 2012; Schoonenboom & Johnson, 2017). An online survey, preceding two focus groups, informed the framing and questions of the focus group (FG) protocol. Quantitative and qualitative data were sequentially collected on participants' awareness of and perspectives on cyberbiosecurity efforts and education within Virginia. The FG elaborated on the outcome of the survey to seek deep qualitative insights from participants. The study design was reviewed and approved by the Virginia Tech Internal Review Board (IRB) under "Exempt" status.

The online survey was conducted through QuestionPro, yielding 35 responses (n=35). Participants responded to questions regarding their stakeholder roles in cyberbiosecurity, perception of Virginia's efforts in cyberbiosecurity education, and perspectives on the National Initiative for Cybersecurity Education (NICE) Workforce Framework relative to Virginia's cyberbiosecurity education. The survey participants had the opportunity to participate in the FG by indicating interest, while also suggesting other potential participants through the survey. Other participants were identified through professional contacts, as highlighted earlier. Consistent with our mixed methodology, new participants other than those in the quantitative survey joined the qualitative strand of the data collection (Creamer, 2017; Malapit et al., 2020). All participants in the FG were provided a copy of the summary of the analysis of the survey data in advance of the FG discussion to acquaint them with the survey outcome and allow them ample time to reflect on the results from their different professional positions. Obtained quantitative data was analyzed and visualized using simple percentages and infographics. The FG transcripts were cleaned, coded, and thematized. Inductive codes were grouped into categories, and themes were generated from those categories. Overall, three themes emerged, which informed the presentation and discussion of the results. Each results section was blended, with qualitative results providing richer insights into the quantitative results.

Like most studies exploring new research areas, the sampling approach creates limitations on extrapolation of findings. While the convenience approach helps to quickly and directly access key stakeholders, its nonprobability nature prevents generalizability of the results. Moreover, the current state of cyberbiosecurity in Virginia may be different from other states, so attempts to extrapolate this study's results should be made with care and understanding of related contexts. Also, the small sample sizes (quantitative and qualitative) limit the potential representation of stakeholders. As a result, important perspectives that might have helped to better improve understanding of the current cyberbiosecurity situation may have been missed. As cyberbiosecurity research and education continue to grow, these limitations will be overcome. Nevertheless, this study serves as one of the foremost empirical attempts at understanding cyberbiosecurity workforce preparation.

Results and Discussion

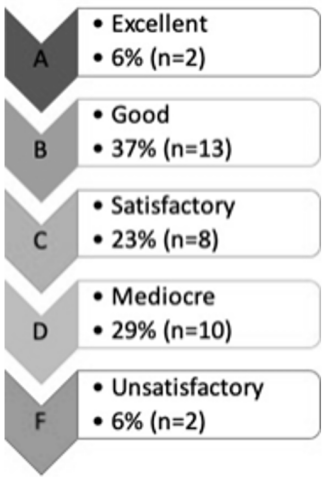
As noted previously, this study sought to synthesize and analyze stakeholders' perceptions in a way that may guide curricular planning for cyberbiosecurity education. We present quantitative findings first, followed by and blended with the qualitative results, which help to provide deeper insights into the quantitative strands of our results. The study being more qualitative heavy (quan → QUAL) and for ease of organization, we organize this results/discussion section under the ensuing themes from the qualitative data analysis: (1) assessing state-level efforts for cyberbiosecurity education, (2) cues from the NICE Framework, and (3) next steps to advance cyberbiosecurity education.

Assessing State-Level Efforts for Cyberbiosecurity Education

Using grade levels of "A" to "F" (Excellent to Unsatisfactory), survey respondents rated Virginia for its efforts to provide appropriate educational opportunities to meet current and future needs (Figure 4).

Figure 4.

Stakeholders' Grading of Virginia's Cyberbiosecurity Efforts



Ratings typically fell within the "B" to "D" range, with only 6% (n=2) identifying Virginia's cyberbiosecurity education efforts as "Excellent" (A) and the same proportion rating the efforts as "Unsatisfactory" (F). Through open-ended questions, respondents revealed that while considerable work has been done so far, the challenge at hand requires greater commitments, particularly in addressing poor awareness and the shortage of educated professionals in cyberbiosecurity, incorporating biosecurity risks in cybersecurity courses, and ultimately dismantling the siloed divide between cybersecurity and biosecurity (Figure 5).

Upon reflecting on the quantitative ranking of Virginia's effort in cyberbiosecurity education, stakeholders in the FGs expressed surprise at the "Good" rating. While stakeholders agreed the rating ("Good") might be a reflection of cybersecurity efforts, they suggested the low but increasing awareness of cyberbiosecurity efforts are lagging behind

Figure 5.

Stakeholders' Comments on State of Cyberbiosecurity Education in Virginia

"Little evidence of biosecurity risks being taught in cybersecurity courses."

"As a high school educator, I have heard almost nothing about it."

"There is no intersection. Both groups (IT and research) remain in silos pursuing their own objectives."

mainstream attention to cybersecurity. One FG participant expressed curiosity: "I mean, just to clarify it was clearly stated that it is about cyberbiosecurity, not about general cybersecurity, because that may be the reason for this kind of, I guess, perception." Another stakeholder opined, "One of the things that I would argue is that cyberbiosecurity stakeholders may not be aware of the problems that they have." These positions strengthen some of the concerns raised in Figure 5. Cybersecurity and biosecurity education are conventionally taught in silos, creating a general challenge of poor awareness of critical issues at the intersection of these fields. Even still, some stakeholders believe there is increasing awareness:

> So, I went to a cyber conference …. And there was a young lady … And she did this wonderful presentation on cyberbiosecurity in the food industry—the whole bit and everything. So, I had her come and talk to my students. And they sat there, and we're just awed … because it had never been brought to the table in that way.

Stakeholders also reported on current efforts to infuse cyberbiosecurity education into existing programs, albeit with some challenges. A participant recounted: "When we review and rewrite these courses, you can do infusion units and add in cyberbiosecurity; or you're going to be like, 'hey, I think this could be a course.'" While the multidimensionality of cyberbiosecurity makes its infusion into existing programs challenging, starting the process of educational awareness needs to begin from somewhere. Spotlighting current cyberbiosecurity education efforts in Virginia, a stakeholder recognizing the marginal efforts so far and using the K-12 cyber education example, reiterated a need for statewide educational programming separate from conventional cybersecurity education:

> The State does a lot of infusions, and cyber is infused across all levels—K through 12—as across all [educational] camps and things like that. But, sometimes I think it [cyberbiosecurity] should be a class within its own, and a lot of those infused units should be classes within their own…. [Even still], just to be able to put it [cyberbiosecurity] in culinary this year was just wonderful.

Cues from NICE Workforce Framework

Among high-level functions associated with the NICE framework (National Initiative for Cybersecurity Careers and Studies [NICCS], n.d.), survey respondents perceived

"protect and defend" (32%) as most deficient (Figure 6). As summarily defined by the NICE Framework, protect and defend is the function category that "identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks" (NICCS, n.d., para. 9). With specialty areas including cyber defense analysis, incident response, and vulnerability assessment and management, organizations would be able to securely protect and defend their internal IT systems against cyberattacks.

However, stakeholders noted that creating awareness is a precursor to protecting and defending critical systems and infrastructures. One FG participant observed: "Cyberbiosecurity needs a lot of awareness about the concept itself, because the large majority of the people do have no notion of it; and that's the reality." Another participant offered a confirmatory statement based on their teaching and research experience: "Without the research projects that Dr. [name concealed] and Dr. [name concealed] conduct, biosecurity and Ag security and critical infrastructure security would not even be offered here in this area."

Moreover, awareness must transcend traditional cybersecurity. While some organizations in need of biosecurity attend to cybersecurity, the effectiveness of such measures remains uncertain. As an example, a stakeholder shared:

> We do occasional phishing campaigns that we run internally, and then we keep track of those results. And we can kind of tweak those dials where we can make very complex phishing campaigns that are difficult to identify or very simple ones to identify. It's a little bit hard to statistically show, you know, performance over time.

Stakeholders suggested that protecting and defending organizational cyberbiosecurity systems is a function of the costs and benefits to the organization and the public. While investing in IT protection and defense is straightforward, the need to go the extra mile to consciously incorporate related components of the biosecurity side will come from the industry seeing a justification of the dollar and cents. This argument boils down to the concern of limited awareness of cyberbiosecurity. Cyberbiosecurity educators and researchers have to demonstrate the cost and benefits to industry leaders. One stakeholder reported: "From previous discussions I've had with respect to industry, sure they have to demonstrate it [cost-benefit]. Why should they [industry] care about this [cyberbiosecurity]? Everything is cost, right? So, what's the cost or benefit?"

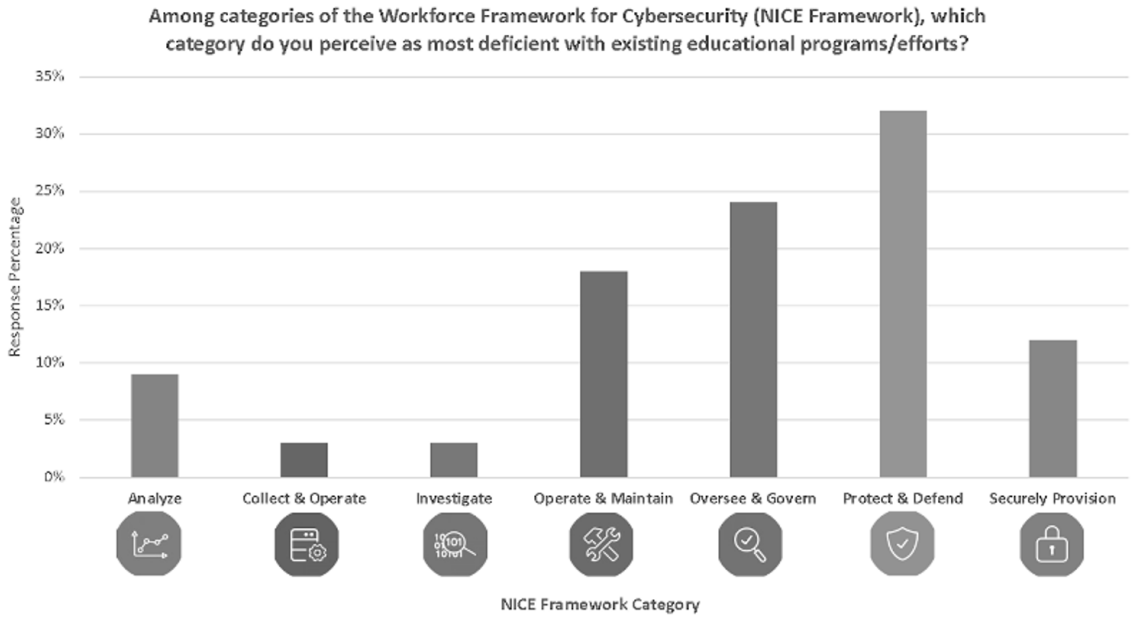
Smaller organizations were considered more problematic, not only with understanding costs and benefits but also being oblivious of the dangers and risks of engaging in cyberspace without measures of protection and defense. Emphasizing this point, a participant shared: "The medium and smaller companies that do bio pharma or biotech research and development, they are completely clueless that anybody's stealing their intellectual property—just that. And what would happen [if it was more], they'd be wiped out." To address this concern, stakeholders believe that development of academia-industry partnerships is key, especially because people in industry may be in a better position to identify vulnerabilities or at least create avenues for better understanding where the challenges lie. A focus group participant advised:

> Have the conversation that 'this is what we're doing; this is what we're thinking about. Here's why it matters to you; here's why you should support it—why you get your staff involved in it. Let us help design education that meets your needs'—that kind of process.

In this way, cyberbiosecurity education programming might comprise both formal and informal components, allowing opportunities for preparing the future workforce and developing the current workforce on-the-job.

Figure 6.

NICE Framework Categories Identified as Most Deficient in Cyberbiosecurity



Next Steps to Advance Cyberbiosecurity Education

Intentional educational opportunities that seek to bridge the siloed gaps were highly recommended. Stakeholders believe that robust cyberbiosecurity education programs would include multiple dimensions, like online learning, interdisciplinary curriculum, systems thinking, and case teaching through cross-disciplinary collaborations. For example, one FG participant said: "One of the easiest ways is to get started with an online package—a few modules, and maybe they are 30 minutes each— 'What is it, and why is it applicable; how can it be used' —a broad array of things." The participant elaborated:

> One of the ingredients to all of this is a knowledge of systems thinking…. You have to be able to integrate your thinking across boundaries and create a functional system…. I've never seen it where one person is capable of doing cyberbiosecurity. It's a team: The bio expert, along with the cyber expert.

Establishing a cooperative effort between the 'bio expert' and the 'cyber expert' is a challenge conveyed in the literature (Cooper, 2015; Richardson, Connell, et al., 2019). This study gives insight into how some of the challenges can be surmounted through industry experience, where the cybersecurity and biosecurity components converge in the form of information technology (IT) and operational technology (OT). One stakeholder shared:

> IT cybersecurity is pretty standard…. The concepts and the basic principles are almost universal, so there are vendors that provide that training…. Then, what I call the OT cyber training, which is more related to the industrial control systems we use here and their cyber components—that training—we have built in-house, because it's pretty customized to what we do. I cannot get it from another vendor, because the truth is, it makes sense only in the sense of our operation.

The cyber component appears to be the easy piece to standardize, but integrating the bio component raises peculiarities that complicate the work. This complication presents conflicts where individuals from the bio and cyber sides are not aware of the inherent concerns (standardization and specialization divide) and the tensions that come with those. If there is not a self and collective awareness of each being, domain experts in cyberbiosecurity may become frustrated in the process of collaborative work. Problematizing the standardization of cyber tools and the specialized protocols of the bio environment as a fulcrum of cyberbiosecurity education programming promises opportunities for ending the long unresolved misunderstanding at the convergence of cybersecurity and biosecurity. This point of convergence holds many promises for education and learning about the cyberbiosecurity threat landscapes.

Consistent with related literature, stakeholders acknowledged that many industrial control systems and parts were not originally designed to be connected to the Internet, which means cybersecurity was not a concern at the time of initial production or installation (Koay et al., 2023; Nawrocki et al., 2020). A participant explained:

> Those devices—industrial control devices—were not originally designed to be connected to the internet and patched and protected and scanned every week or month. So as they're interconnecting them to the networks, these devices are kind of left behind, and they're not constantly having firmware upgrades, system upgrades; so they're extremely vulnerable to these attackers.

Here, biosecurity professionals who use industrial control systems are not as likely to be protected with the most current cybersecurity. While specialized protections may be implemented in some parts of a system, the overall protection depends on the strength of the weakest component. These concerns confirm Richardson, Connell, et al.'s (2019) position that neither the cyber expert nor bio expert has the agency to successfully address cyberbiosecurity challenges. However, some stakeholders were able to share examples of successful collaboration. For example, one FG participant shared:

> We have a group of process engineers—the experts playing with chemicals and sludge and making sure the combinations are right for them.… These guys sit down with the IT—or control systems engineers—and they came up with a class—a 30-minute class. And we make sure every single person that uses our systems goes through that class. The goal is not to make them an expert; the goal is to make them aware of this risk.

The participant expanded:

> The interesting part is, that element is relatively new. We have audits every now and then. In the previous audits, that was not identified as a problem; you know, the training was—they always required just IT training—cyber IT. During the last audit cycle, the auditors—which are people I consider to be very competent, very specialized in cyber threats—they told us, 'Look guys, now that's not enough; you have to go into the IoT [Internet of Things] side.' So it's more like it, somehow, it gets into the biosecurity component, and you have to include that in your training; and that's why we're including it now. I suspect that over time we're going to improve and to refine it, but it's something that we started just last year.

A call for collaboration remains an ultimate call in cyberbiosecurity education programming and workforce development. "The solution set is not simply technical: creating cross-sector convergence opportunities for effective communication and collaboration as well as governance, policy, and regulatory structures is also necessary" (Richardson, Connell, et al., 2019, p. 2).

Conclusions and Implications

Automation and digitization in agriculture and life sciences have marked impacts on how items in the biosphere are produced, processed, and supplied, as well as opportunities for disease diagnosis, prevention, and cure (Subeesh & Mehta, 2021). However, the accompanying

proliferation of cyber-physical systems increases the chances of cyberattacks on agriculture and life sciences systems (Titus et al., 2023). Despite similar foci on protection and security, addressing emerging challenges at the intersections of cybersecurity and biosecurity is difficult, as each field has different domain knowledge and therefore focuses on different aspects of the threats (Duncan et al., 2021; Richardson, Conell, et al., 2019). Cyberbiosecurity is an emerging field at the interface of the life sciences and digital world that seeks to understand the intersections to enable domain experts to make the most of the digital revolution while protecting and securing the confidentiality, integrity, and availability of critical biological data and infrastructure from bad cyber actors (Greenbaum, 2023; Murch, 2023).

This study was designed to identify opportunities for specialized career development and mechanisms for integrated cyberbiosecurity education. In analyzing stakeholders' perceptions to inform curricular planning for cyberbiosecurity education, we encountered the challenge of the field being relatively new, lacking established signature pedagogies. Consequently, there is a scarcity of educational resources showcasing current practices in cyberbiosecurity. This study focused on what professionals at the intersection of cybersecurity and biosecurity "do, think, and value" and analyzed various perspectives as a foundation for developing signature pedagogies in cyberbiosecurity. We used a sequential explanatory mixed methods design with a qualitative priority and a convenience sampling approach to reach targeted stakeholders in Virginia.

The limited awareness and understanding of cyberbiosecurity issues contribute to educational gaps in this field. Cybersecurity and biosecurity—as broad disciplines—often operate in separate silos, each focused on distinct objectives (Murch & DiEuliis, 2019). They lack the collective agency needed to effectively address the rising concerns at the convergence of these disciplines within cyberbiosecurity. While opportunities are available for infusing cyberbiosecurity into existing cyber courses, the multidimensionality of cyberbiosecurity makes infusion challenging. Robust cyberbiosecurity education programming should consider multiple dimensions, including online learning, interdisciplinary curriculum, systems thinking, and case teaching through cross-disciplinary collaborations. We identified a standardization and specialization divide as one source of tension among cyber and bio professionals, fostering the reluctance to cooperate. In designing education programs for workforce preparation, the standardization of cyber tools and the specialized protocol of the bio environment should serve as an important foundation for building other relevant elements. The "protect and defend" category of the NICE Framework was highlighted as the most deficient high-level function in cyberbiosecurity. To address this deficiency, it is crucial to promote awareness of cyberbiosecurity issues and establish partnerships with industries operating within the convergence domain. Educators and researchers play a pivotal role in fostering this engagement by effectively demonstrating to industry leaders the added costs and benefits of implementing cyberbiosecurity measures.

Overall, there is a need for the infusion of cyberbiosecurity fundamentals into existing agriculture and life science courses/programs to increase awareness, using a systems thinking approach to draw connections to

Table 1.

Cyberbiosecurity Workforce Development Curricular Resources

Resource Title	URL
CyberBiosecurity Training Module for Life Science	https://osf.io/63agh/wiki/home/?view_only=8a829e39cf474b62a0f4336880ca8f5d
Cybersecurity in Food and Agriculture, Advanced	https://www.cteresource.org/career-clusters/agriculture-food-natural-resources/cybersecurity-in-food-and-agriculture-advanced/
Improving Cybersecurity Information: Cybersecurity for Iowa Farmers and Rural Businesses	https://www.extension.iastate.edu/agdm/info/cybersecurity.html
Integrating Cybersecurity and Agricultural Innovation	http://hdl.handle.net/10919/111501
Interdisciplinary approach to experiential learning in cyberbiosecurity and agriculture through workforce development	https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/2
Leadership for CyberBioSecurity: The Case of Oldsmar Water	http://hdl.handle.net/10919/113624
Securing the Food Industry: An Introduction to Cyberbiosecurity for Food Science	http://hdl.handle.net/10919/111375

pertinent emerging concerns in the cyberbiosecurity threat landscape (Drape & Murch, 2022). To enhance educational opportunities for both college learners and industry professionals, education programming should include short online modules that cater to different categories of learners. This approach ensures ease of access and accommodates the needs of various individuals. Furthermore, fostering continuous interdisciplinary collaboration and academia-industry partnerships is essential for creating awareness and developing robust cyberbiosecurity education. These initiatives are vital for equipping the future workforce and providing professional on-the-job training for the current workforce. Cyberbiosecurity education programming efforts should explore the standardization of cyber tools and the customization of those tools to the bio environment as a critical point of integration in cyberbiosecurity.

More empirical research is needed to explore cyberbiosecurity education programming and workforce preparation. Future research may consider reaching a larger sample of cyberbiosecurity educators, researchers, and practitioners to better facilitate the extrapolation of findings. While this work has identified some of the general issues underlying cyberbiosecurity education programming, further studies may look at specifics related to how an actual curriculum or course may be sequenced, balanced, and adaptable to contemporary realities. In the mid and longer terms, efforts should be geared toward developing cyberbiosecurity education into full-fledged certificate or degree programs. For educators who are ready to begin infusing cyberbiosecurity into their courses and programs, existing resources may be useful (see Table 1).

References

Adeoye, S., & Kaufman, E. (2023). Co-generative learning: Applying the undisguised case teaching method. *Conference on Higher Education Pedagogy 2023*, 75-76. http://hdl.handle.net/10919/114242

Adeoye, S., Kaufman, E. K., Brown, A. M., & Batarseh, F. A. (2023, April 18). *Mapping the landscape of cyberbiosecurity education* [Conference session]. Commonwealth Cyber Initiative Symposium, Richmond VA, United States. http://hdl.handle.net/10919/114739

AI EdgeLabs. (2022, July 06). *Cyber attacks on the rise in the agriculture industry*. https://edgelabs.ai/blog/cyber-attacks-on-the-rise-in-the-agriculture-industry/

Beck, D., & Eno, J. (2012). Signature pedagogy: A literature review of social studies and technology research. *Computers in the Schools*, *29*, 70-94. https://doi.org/10.1080/07380569.2012.658347

Berger, K. M., & Schneck, P. A. (2019). National and transnational security implications of asymmetric access to and use of biological data. *Frontiers in Bioengineering and Biotechnology*, *7*(21), 1-7. https://doi.org/10.3389/fbioe.2019.00021

Bryne, J. (2019, October). *Agriculture is the least digitized sector globally, so it is ripe for disruption, says Alltech*. https://www.feednavigator.com/Article/2019/10/22/Agriculture-is-ripe-for-disruption

Calder, L. (2006). Uncoverage: Toward a signature pedagogy for the history survey. *The Journal of American History*, *92*(4), 1358-1370. https://doi.org/10.2307/4485896

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 (Eds.). *Proceedings of the 12th International Conference on Cyber Warfare and Security*, 90-95.

Colorado State University. (n.d.). *Bio-cybersecurity at CSU*. https://www.research.colostate.edu/bio-cybersecurity/#

Cooper, C. (2015). *Cybersecurity in food and agriculture*. In J. LeClair (Ed.), Protecting our future (Vol. 2, Ch. 7). Hudson Whitman.

Crawford, P., & Fink, W. (2019). Employability skills and students critical growth areas. *NACTA Journal*, *64*, 132-141. https://www.jstor.org/stable/27157784

Creamer, E. G. (2017). *An introduction to fully integrated mixed methods research*. Sage.

Degreenia, A., & Sutton, R. (2020). An inquiry into the professional and leadership skills that employers in agricultural private and public sectors value in new graduates. *NACTA Journal*, *65*, 73-91. https://www.nactateachers.org/attachments/article/3072/2020-0295%20FINAL.pdf

DiEuliis, D. (2023). Revisiting the digital biosecurity landscape. In D. Greenbaum (Ed.), *Cyberbiosecurity* (pp. 71-78). Springer. https://doi.org//10.1007/978-3-031-26034-6_5

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. *Frontiers in Bioengineering and Biotechnology*, *9*, 737927. https://doi.org/10.3389/fbioe.2021.737927

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

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, *7*, 63. https://doi.org/10.3389/fbioe.2019.00063

Duncan, S., Carneiro, R., Braley, J., Hersh, M., Ramsey, F., & Murch, R. (2021). Beyond ransomware: Securing the digital food chain. *Food Technology Magazine*, 75(9). https://www.ift.org/news-and-publications/food-technology-magazine/issues/2021/october/features/digital-food-chain

Emerson, R. W. (2021). Convenience sampling revisited: Embracing its limitations thoughtful study design. *Journal of Visual Impairment and Blindness*, *115*(1), 76-77. https://doi.org/10.1177/0145482X20987707

Federal Bureau of Investigation. (2016, March 31). Smart farming may increase cyber targeting against US food and agriculture sector. *Private Industry Notification*, 160331-001. https://publicintelligence.net/fbi-smart-farm-hacking/

Federal Bureau of Investigation. (2021, September 1). Cyber criminal actors targeting the food and agriculture sector with ransomware attacks. *Private Industry Notification*, *20210901-001*. https://www.ic3.gov/Media/News/2021/210907.pdf

Federal Bureau of Investigation. (2022, April 20). Ransomware attacks on agricultural cooperatives potentially timed to critical seasons. *Private Industry Notification, 20220420-001*. https://www.ic3.gov/Media/News/2022/220420-2.pdf

Federal Bureau of Investigation (FBI), Food and Drug Administration Office of Criminal Investigations (FDA OCI), & US Department of Agriculture (USDA). (2022, December 15). Criminal actors use business email compromise to steal large shipments of food products and ingredients. *Joint Cybersecurity Advisory, AA22-340A*. https://www.ic3.gov/Media/News/2022/221216.pdf

Freyhof, M., Grispos, G., Pitla, S., & Stolle, C. (2022). Towards a cybersecurity testbed for agricultural vehicles and environments. *arXiv:2205.05866*. https://doi.org/10.48550/arXiv.2205.05866

Greenbaum, D. (2023). The convergence of biotechnology and cybersecurity: A primer on the emerging field of cyberbiosecurity. In D. Greenbaum (Ed.), *Cyberbiosecurity* (pp. 1-6). Springer. https://doi.org/10.1007/978-3-031-26034-6_1

Guest, G. (2012). Describing mixed methods research: An alternative to typologies. *Journal of Mixed Methods Research*, *7*(2), 141-151. https://doi.org/10.1177/1558689812461179

Jager, J., Putnick, D. L., & Bornstein, M. H. (2017). More than just convenience: The scientific merits of homogeneous convenience samples. *Monographs of the Society for Research in Child Development*, *82*(2), 13-30. https://doi.org/10.1111/mono.12296

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. *Current Opinion in Biotechnology*, *70*, 15-22. https://doi.org/10.1016/j.copbio.2020.09.003

Kaufman, E., & Adeoye, S. (2023). Enhancing learning through undisguised teaching case studies: Both instructor-facilitated and student-written. *Proceedings of the American Association for Agricultural Education Southern Region (AAAE-SR)*. http://hdl.handle.net/10919/114241

Koay, A. M. Y., Ko, R. K. L., Hettema, H., & Radke, K. (2023). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. *Journal of Intelligent Information Systems, 60*, 377-405. https://doi.org/10.1007/s10844-022-00753-1

MacIntyre, C. R., Engells, T. E., Scotch, M., Heslop, D. J., Gumel, A. B., Poste, G., Chen, X., Herche, W., Steinhöfel, K., Lim, S., & Broom, A. (2018). Converging and emerging threats to health security. *Environments Systems and Decisions, 38*, 198-207. https://doi.org/10.1007/s10669-017-9667-0

Malapit, H., Ragasa, C., Martinez, E. M., Rubin, D., Seymour, G., Quisumbing, A. (2020). Empowerment in agricultural value chains: Mixed methods evidence from the Philippines. *Journal of Rural Studies*, *76*, 240-253. https://doi.org/10.1016/j.jrurstud.2020.04.003

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

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

Murch, R., & DiEuliis, D. (2019). Editorial: mapping the cyberbiosecurity enterprise. *Frontiers in Bioengineering and Biotechnology*, *7*(235), 10-3389. https://doi.org/10.3389/fbioe.2019.00235

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.2018.000

Nawrocki, M., Schmidt, T. C., & Wahlisch, M. (2020). Uncovering vulnerable industrial control systems from the internet core. *Proceedings of 17th IEEE/IFIP Network Operations and Management Symposium (NOMS)*. https://doi.org/10.48550/arXiv.1901.04411

National Initiative for Cybersecurity Careers and Studies. (n.d.). *Workforce framework for cybersecurity (NICE Framework)*. https://niccs.cisa.gov/workforce-development/nice-framework#

Nikander, J., Mnninen, O., & Laajalahti, M. (2020). Requirements for cybersecurity in agricultural communication networks. *Computer and Electronics in Agriculture*, *179*, 105776. https://doi.org/10.1016/j.compag.2020.105776

Pauwels, E. (2021, May). *Cyber-biosecurity: How to protect biotechnology from adversarial AI attacks* [Strategic Analysis 26]. Hybrid CoE. https://www.hybridcoe.fi/publications/cyberbiosecurity-how-to-protect-biotechnology-from-adversarial-ai-attacks/

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. *Materials Today: Proceedings*, *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. (2019). Cyberbiosecurity: A call for cooperation in a new threat landscape. *Frontiers in Bioengineering and Biotechnology*, *7*(99), 1-5. https://doi.org/10.3389/fbioe.2019.00099

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building capacity for cyberbiosecurity training. *Frontiers in Bioengineering and Biotechnology*, *7*(122), 1-5. https://doi.org/10.3389/fbioe.2019.00112

Sayers, R. G., Sayers, G. P., Mee, J. F., Good, M., Bermingham, M. L., Grant, J., & Dillon, P. G. (2013). Implementing biosecurity measures on dairy farms in Ireland. *The Veterinary Journal*, *197* (2), 259-267. https://doi.org/10.1016/j.tvjl.2012.11.017

Schoonenboom, J. & Johnson, R. B. (2017). How to construct a mixed methods research design. *Köln Z Soziol*, *69*(suppl 2), 107-131. https://doi.org/10.1007/s11577-017-0454-1

Shulman, L. S. (2005). Signature pedagogies in the professions. *Daedalus*, *134*(3), 52-59. https://www.jstor.org/stable/20027998

Sinha, B. B., & Dhanalakshmi, R. (2022). Recent advancements and challenges of Internet of Things in smart agriculture: A survey. *Future Generation Computer Systems*, *126*, 169-184. https://doi.org/10.1016/j.future.2021.08.006

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* (pp. 217-263). Springer. https://doi.org/10.1007/978-3-031-26034-6_13

Stephen, S., Alexander, K., Potter, L., & Palmer, X. -L. (2023). Implications of cyberbiosecurity in advanced agriculture. *Proceedings of the 18th International Conference on Cyber Warfare and Security*, 387-393. https://papers.academic-conferences.org/index.php/iccws/article/view/995/977

Subeesh A., & Mehta, C. R. (2021). Automation and digitization of agriculture using artificial intelligence and internet of things. *Artificial Intelligence in Agriculture*, *5*, 278-291. https://doi.org/10.1016/j.aiia.2021.11.004

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

van der Ham, J. (2021). Toward a better understanding of "cybersecurity." *Digital Threats: Research and Practice*, *2*(3), Article 18. https://doi.org/10.1145/3442445

Waage, J. K., & Mumford, J. D. (2008). Agricultural biosecurity. *Philosophical Transactions of the Royal Society*, *363*, 863-896. https://doi.org/10.1098/rstb.2007.2188

Walsh, P. F. (2022). Securing the bioeconomy: Exploring the role of cyberbiosecurity. In M. Gill (Ed.), *The Handbook of Security* (pp. 335-355). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-91735-7_16

Watson, A., Migliaccio, K., & Porter, W. (2019). Alumni, faculty, and employer insights into agricultural operations management curricula. *NACTA Journal*, *64*, 224-235. https://www.jstor.org/stable/27157797

Wayne, J., Raskin, M., & Bogo, M. (2010). Field education as the signature pedagogy of social work education. *Journal of Social Work Education*, *46*(3), 327-339. https://www.jstor.org/stable/23044417

Yeboah-Boateng, E. O. (2013). *Cyber-security challenges with SMEs in developing economies: Issues of Confidentiality, Integrity & Availability* (CIA). Institute for Elektroniske Systemer, Aalborg Universitet.