Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Biosafety and Health 3 (2021) 11–21

Contents lists available at ScienceDirect

Biosafety and Health

journal homepage: www.elsevier.com/locate/bsheal

Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?

Siguna Mueller *

Multidisciplinary, Independent Researcher, Austria

ARTICLE INFO

Article history:
Received 26 April 2020
Received in revised form 17 September 2020
Accepted 23 September 2020
Available online 25 September 2020

Keywords:
Laboratory safety
Cyberbiosecurity
Risk assessment
Protective measures
Convergence
Biolabs of the future

ABSTRACT

As the entire world is under the grip of the coronavirus disease 2019 (COVID-19), and as many are eagerly trying to explain the origins of the virus and cause of the pandemic, it is imperative to place more attention on related potential biosafety risks. Biology and biotechnology have changed dramatically during the last ten years or so. Their reliance on digitization, automation, and their cyber-overlaps have created new vulnerabilities for unintended consequences and potentials for intended exploitation that are mostly under-appreciated. This study summarizes and elaborates on these new cyberbiosecurity challenges, (1) in terms of comprehending the evolving threat landscape and determining new risk potentials, (2) in developing adequate safeguarding measures, their validation and implementation, and (3) specific critical risks and consequences, many of them unique to the life-sciences. Drawing other's expertise and my previous work, this article reviews and critically interprets our current bio-economy situation. The goal is not to attribute causative aspects of past biosafety or biosecurity events, but to highlight the fact that the bioeconomy harbors unique features that have to be more critically assessed for their potential to unintentionally cause harm to human health or environment, or to be re-tasked with an intention to cause harm. It is concluded with recommendations that will need to be considered to help ensure converging and emerging biorisk challenges, in order to minimize vulnerabilities to the life-science enterprise, public health, and national security.

1. Motivation

Ever since the coronavirus disease 2019 (COVID-19) pandemic, (laboratory) biosafety and biosecurity concerns are even more rigorously scrutinized. This article uses the current pandemic lens to evaluate biological risks from biological research, particularly those amplified by the digitization of biological information and biotechnology automation.

The cyberphysical nature of biotechnology has led to fascinating advances throughout the bioscience field. Concerns have recently been raised regarding new risks that may lead to unintended consequences or unrecognized potentials for misuse. Just as the emergence of the Internet some decades ago led to a major revolution and by necessity, was complemented by the field of Cybersecurity - we are now facing the era of cyber biosecurity[1] with its own security vulnerabilities.

The DNA synthesis industry has worked proactively for many years to ensure that synthesis is carried out securely and safely.[2] These efforts have been complemented by the growing desire and capability to resynthesize biological material using digital resources [1,2]. Nevertheless, the convergence of technologies at the nexus of life and medical sciences, cyber, cyberphysical, supply chain and infrastructure systems [3], has led to new security problems that have remained elusive to the majority of the scientific, agricultural, and health communities. It has only been during the last few years that awareness of these new types of vulnerabilities is growing, especially related to the danger of intentional manipulations.

As these concerns have spawned the emergence of cyberbiosecurity as a new discipline, it is essential to realize that its focus is not merely on traditional cyber-attacks (Section 2 and Fig. 1 below). Due to the increased reliance of the bioscience fields on cyberphysical systems (CPS, Fig. 3 below), potentials for exploitation exist at each point where bioengineered or biomanufactured processes or services interface the cyber and the physical domain. Thereby, attackers may exploit unsecured networks and remotely manipulate biologic data, exploit biologic agents, or affect physical processing involving biological materials. which may result (whether intentionally or unintentionally) in unwanted or dangerous biological outcomes [4–7].

Great efforts have been put into place rigorously to assess the new risks and threats (see in particular [3] and the recent National Academy of Sciences, Engineering, and Medicine report “Safeguarding the Bioeconomy” [7, pp. 204–211]). Nonetheless, cyberbiosecurity is still in its infancy. There is still limited expertise to fully characterize and assess the emerging

* Corresponding author: Multidisciplinary, Independent Researcher, Austria.
E-mail address: siguna.mueller@protonmail.com.

[1] Informally, cyberbiosecurity is the discipline at the interface of (1) biosafety/biosecurity, (2) cybersecurity, and (3) cyberphysical security. For more details, see Section 2 below.

[2] In contrast to safety considerations - which analyze how a product or service might accidentally harm the research him/herself or others - security concerns consider how something could be used to harm others intentionally.

http://dx.doi.org/10.1016/j.bsheal.2020.09.007

cyberbio risks [8], and it has been recognized that generic cyber and information security measures are insufficient [8–14].

Triggered by the COVID-19 pandemic, enormous amounts of resources have been devoted to identify its exact genesis. This article aims to challenge this narrow focus by concentrating on the broader context of cyberbiosecurity, to illuminate serious new concerns for a broad audience. Distinct challenges will be highlighted and specific steps to help support risk deterrence efforts suggested.

2. The uniqueness and challenge of cyberbio protection

Most broadly, cyberbiosecurity aims to identify and mitigate security risks fostered by the digitization of biology and biotechnology automation. Fig. 1 gives a summary of how this new paradigm evolved. While others, including the author, began to investigate these challenges almost a decade ago [13,15–18], the term cyberbiosecurity was first (informally) used in an article published in 2018 [19]. These authors warned of security issues resulting from the bioeconomy's cyberphysical interface, as it was recognized that all biomanufacturing processes are, in fact, CPS (see also Fig. 3 below). A preliminary definition of cyberbiosecurity (Fig. 1, orange circle) from the traditional 'security' perspective (footnote 3) was given by Murch et al. [4] who considered cyberbiosecurity[3] to be at the interface of (1) biosecurity, (2) cybersecurity, and (3) cyberphysical security. Consequently, the notion 'cyberbiosafety' was introduced in [20] as "the cyber vulnerabilities associated with networked data systems, laboratory equipment and facility security and engineering controls that may result in environmental contamination or pose a threat to the health of humans, animals. and plants including the health of building occupants, the surrounding community, and/or users and consumers of products created by the life science enterprise." Apparently, this fact motivated a modification of the previous working definition of cyberbiosecurity - which in [21] was extended to include biosecurity and biosafety. It is worthwhile to mention that CPS has blurred the lines between safety and security, and even in the cyberfields, these terms are more often used interchangeably. The same way, cyberbiosecurity utilizes this notion to include the full range of vulnerabilities as first described in [19] most broadly as "understanding the new risks emerging at the frontier between cyberspace and biology."

It is important to realize that it is not only about cyber-security and biosafety/biosecurity. Many of the massive problems arise due to the convergence of these fields. The cyberphysical nature of biotechnology raises unprecedented issues, related to unintended consequences and intended actions. Table 1 summarizes the scope and impact of the new risks throughout the life-science field, as described in the literature since the recent launching of the cyberbiosecurity paradigm. The (sometimes hypothesized) scenarios depicted in the table often point to several weaknesses and thereby make them susceptible to more than one form of attack (e.g., traditional cyber crime or attacks targeting CPS). The last column in the table highlights the types of attack these situations are most vulnerable to.

Cyberbio risks range from the victim organizations unwittingly producing high-consequence biological agents to the corruption of safety and security ensuring processes, with possibly hazardous downstream consequences affecting a broad spectrum of critical infrastructure sectors (Fig. 2). In addition to consequences endangering public health, the environment, economy, and national security, the range of risks and threats can include sequestration of information for military and intellectual property purposes, which could be turned into economic warfare. An interplay of several factors enhances these new dangers:

[3] Concretely, these authors defined cyberbiosecurity as "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience."

2.1. Less reliance on tacit knowledge

Traditionally, life-science research has required particular expertise and technical skills tobe learned through constant practice and peers' observation. This process has led to the misconception that the life-science fields are shielded from malicious interventions. Moreover, the bioeconomy industry mitigates risks for intended attacks and unintended consequences through many control and quality assurance strategies. Many of these processes are now CPS (Fig. 3). However, due to the potentially high-consequence dependency between physical systems and the special-purpose computers that control and monitor them, CPS is susceptible to various security risks and threats. Thus, the reliance on CPS may enable new forms of attack that circumvent traditional tacit knowledge and exploit unknown vulnerabilities at the cyber-interface.

2.2. Incomplete awareness

During the last few years, the biotechnology industry has fallen prey to severe attacks (see e.g. [7, Table 7–1]), although there is no broad awareness of this. This critical observation and the compelling need to question the "naive trust" throughout the life-science arena were key drivers to establish cyberbiosecurity as a new discipline [19]. Additional sobering criminal cases that have affected the bioscience field are now emerging, even during the current pandemic (e.g. [10,20,22–25]). As noted in [22], these encompass three critical areas of attack - sabotage, corporate espionage, and crime/extortion. However, people in the life-sciences are mostly ignorant of the dangers as they are barely trained in security issues - or not at all. Research and healthcare industries are vulnerable to cyberbiosecurity attacks because they have not kept up with threats [8,26].

2.3. Capitalizing on a common misconception

Generally, it is widely accepted that cybersecurity attacks and data breaches are a matter of when, not if. Very recently, ransomware attacks have been recognized as "the primary threat" to healthcare organizations [27]. Statements like these seem to support the understanding that cyberbio concerns in the bioeconomy could be dealt with IT solutions alone (and possibly optimized for life-science demands). Unfortunately, the reliance on CPS generates unrecognized convergence issues. It is essentialto understand that due to cross-over effects, neither cyber nor physical security concepts alone are sufficient to protect a CPS. "Separate sets of vulnerabilities on the cyber and physical sides do not simply add up, they multiply" [28]. Notably, cyber-attacks on critical automated (computer-based) processes (e.g., workflow or process controls) may lead to dire real-world consequences, similar to direct physical attacks. For instance, a 2008 explosion in the highly secure 1,099- mile Baku-Tbilisi-Ceyhan pipeline was caused by computer sabotage. The primary weapon for this cyberphysical act of terrorism was "a keyboard" [28,29]. In general, the term 'physical' in CPS (Fig. 3, central box) is applied to the 'engineering, physical and biological' [30] components of the system, or more generally, any components of the physical world which are connected through cyber elements. Unfortunately, security dangers involving the 'biological' aspects have received little attention. Notably, in the context of the life-sciences, any CPS may alter biological properties. A compromise to CPS may lead to situations such as the "faulty or even dangerous synthesis of biomaterials or interference with biological containment systems" [7]. It is also important to understand that in addition to general CPS challenges, the biological sciences framework leads to other concerns that have not been adequately assessed (Section 4 and Fig. 3, right arrow).

2.4. A gap in expertise

As with all converging areas, expertise is usually very hard to come by (see also Table 1). A very recent study that researched the opinion of international field leaders in biotechnology and cybersecurity concluded that "the issue of cyberbiosecurity is not well-known or

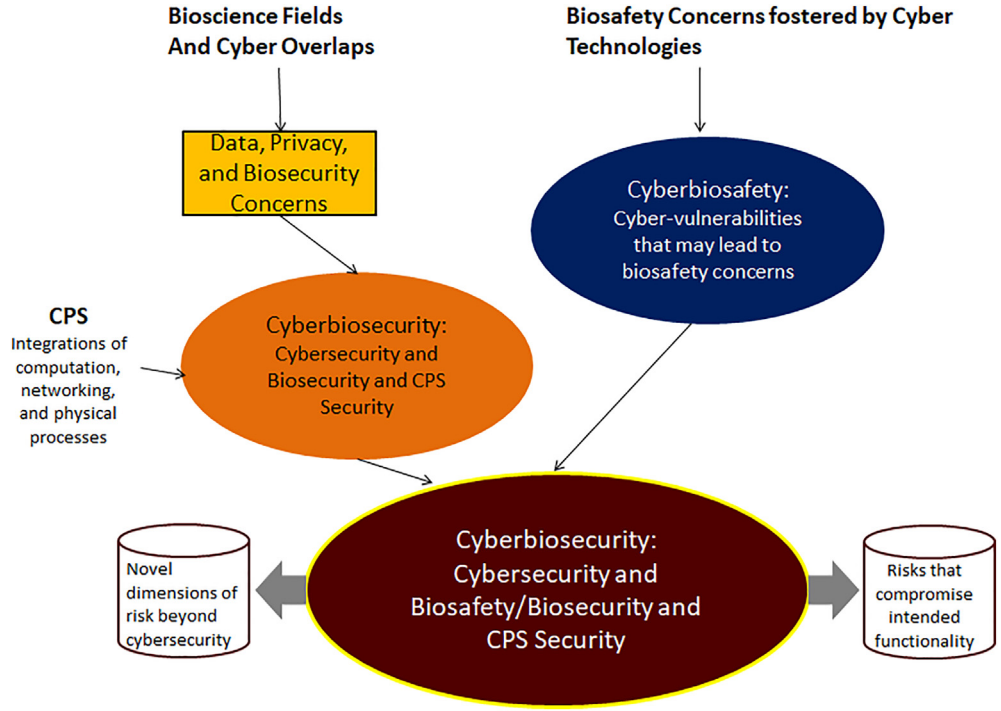

Fig. 1. Emergence and scope of cyberbiosecurity. The figure depicts the core pillars that have become a part of this new discipline. The definitions of these terms are given in Section 2.

understood, even among biotechnology and cybersecurity experts" and "Biotech does not think about security other than more traditional biosecurity and biosafety… security communities do not understand biotech" [8]. All this is compounded by the fact that "Extant legislation addressing cyber- and biological risks lags behind technological advances in these fields and cannot be depended upon to address combined cyberbiological threats, vulnerabilities, and consequences" [11].

3. Challenges with risk assessment and solutions

3.1. No clear cyberbiosecurity risk and threat assessment

Any reasonable risk management system will endeavor to develop a clear understanding of existing risks and threats, what could happen within a framework of specific circumstances, how and to what degree this could be mitigated, and which resources, interventions, and steps are required. Generally, in the life sciences, "Risk assessment of public harm is challenging because it necessitates consideration of the intent and capability of those who wish to do harm, as well as the vulnerability of the public and the status of public health preparedness for both deliberate and accidental events" [31].

An important initial step in effectively managing risk is to develop a comprehensive understanding of vulnerabilities [5]. With cyberbiosecurity, these efforts are still in their infancy. A key finding of a recent Frontiers Research Topic [32] was that "mapping the topology of cyberbiosecurity has just begun…"

The first-ever cyberbiosecurity analysis was conducted by identifying critical threats and their impacts in a specific manufacturing facility [4, Fig. 1]. To extend this approach, it has been suggested to start with a certain sector, such as the food and agriculture (Fd + Ag) branch, biopharmaceutical manufacturing, or laboratories [20,22,33,34], and assess the risks relative to that particular industry or discipline.

While in some situations, specific hazard analysis systems and risk scales have proven useful (e.g. the Hazard Analysis Control Point system for the Fd + Ag sector or, more generally, the Infrastructure Survey Tool [35] or NIST guidelines [36]), it is recognized that fully scoping all the cyberbio risks, not to mention their relative likelihood and impact, is rather challenging [8,21,22]. Although some of the cyberbio vulnerabilities share compelling similarities to the early days of the Internet [37], there are critical differences [9–12,14].

3.2. Challenges in developing a solution

While most responders to the above-mentioned survey of international experts [8] agreed that their organizations had "considered" cyberbio issues, some noted "insufficient time" or "no idea" how to address them, and all pinpointed the lack of available resources. This section describes some of the difficulties.

- The problem of identifying what needs to be protected:
  - Many of the novel cyberbio risks and threats (Table 1) have not been fully scoped. They are difficult to characterize, and envisioning the complete risk landscape continues to be a challenge [8,14,22,38,39].
  - Identifying and hierarchizing the extent, impact and severity of various (including, hypothetical) new vulnerabilities is difficult.
  - There is no comprehensive model to effectively capture, assess, and address the motivations, capabilities, and approaches of those who may cause harm (see also Section 4.2).

- How protection is achieved and enforced:
  - Existing solutions from the cyber domain are only geared at specific aspects of biosecurity and cybersecurity but do not address the overlap and the issues arising from this convergence [8,14,39].
  - Due to variations in types of threats, targets and potential impacts, it is not straightforward to determine a possible solution's applicability and effectiveness.
  - As "there is no one model" to secure the use of information systems across the bioeconomy [7], weak or premature solutions may only help address a distinct problem but be misapplied in a different context, or even become a source for exploitation (Section 4.2 and Fig. 4 below).

Table 1
Scope and impact of cyberbiosecurity risk.

Area of biorisk concern	Description of dangers/consequences[a]	Source	Major attack potential[b]
General scope and consequences	"Trust within the biotechnology community creates vulnerabilities at the interface between cyberspace and biology." Data, bioinformatic input tools or industrial process control systems used by a biotech facility may be "vulnerable to tampering, which could result in damage to the facility or the subversion or sabotage of its products, and subsequent harm to people, plants, animals, or the environment."	[7,19]	C,CP
	In spite of broad efforts to safeguard the bioeconomy in recent years, "the 'cyber' overlaps with biosecurity have not been realized or fleshed out." This creates vulnerabilities at the "interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems."	[4]	V
	Cyberbio concerns "include occupational hazards, damage to equipment, batch failure leading to loss of product, and theft of IP… Shortages or stock-outs of medicines… financial burden..."	[22]	V
	Adverse consequences include "the disabling or disruption of important systems or infrastructure leading to disruption of commercial operations or impeding good manufacturing practices...."	[8]	C,CP
	"Cyber-physical systems pose significant security and safety risks since their compromise can have effects on the real world; in this case, those effects could include faulty or even dangerous synthesis of biomaterials or interference with biological containment systems…corruption of environmentally or health related sensors or data could result in the misapplication of health care or environmental remediation."	[7]	CP
National and transnational	"Intellectual property and proprietary information losses associated with digitized biological information could rise to the millions or billions, eventually resulting in economic decreases and reduced international competitiveness (Heus et al., 2017)."	[11]	V
	"Other national security concerns include loss of privacy, discrimination, data loss or theft, industrial and commercial sabotage, industrial hacking, exploitation of research to increase disease severity, targeting based on specific DNA patterns, and the production of dangerous and novel pathogens without physical samples (Bajema et al., 2018)."	ibid.	V
	Referring to critical infrastructure sectors: "While some may be aware of the cyberbiological risk to their sectors, they have not yet determined how best to defend against individual cyber- and biological, let alone combined cyberbiological, risks."	ibid.	V
Biopharma, biological therapies, public Health	"Biopharmaceutical companies employ cyber-physical systems across a range of functions: raw materials sourcing, cell line development and optimization, upstream and downstream process development, manufacturing, validation studies, clinical trials, supply chain management of products, post-market drug safety monitoring, and interfacing with health providers."	[22]	CP
	"Cyberbiosecurity breaches could directly impact patients, from compromised data privacy to disruptions in production that jeopardize global pandemic response."	ibid.	V
	"The intellectual property, manufacturing processes, regulatory requirements and sophisticated cyber-physical systems involved in the production of biologic therapies may be particularly vulnerable to three major forms of cyberattacks: sabotage (deliberate and malicious acts that damage digital or physical infrastructure), corporate espionage (gaining access to sensitive information to attain advantage over an adversary), and crime/extortion (encrypting files with a ransom note asking for remuneration for their return) (Morag, 2014)."	ibid.	V
Biological databases	"The more we rely on genome databases, the more likely these databases will become targets for cyber-attacks to interfere with public health and biosecurity systems by compromising their integrity, taking them hostage, or manipulating the data they contain."	[12]	C
	"Many web sites provide methods for users to upload data. Interestingly, there seems to be no case where the data integrity is checked during the transfer process...."	ibid.	C
	"Existing cyberattack methods could easily target current molecular databases… Almost all traditional cybersecurity solutions fail at data volume, velocity, and variety of this scale… verifying the validity of the data is particularly challenging and cannot be easily performed using existing methods."	ibid.	C
	"Errors may also be intentionally introduced into a biological database… depending on how sequences could be submitted to the database, the adversary may be able to keep the pathogenic sequence from being detected by certain anomaly detection heuristics."	[37]	C, U
Synthetic biology	"Commercially-available customer screening solutions still require a great deal of manual review of false positive findings… Current sequence screening algorithms are computationally expensive and, given the high false positive rate, the results of sequence screening can be complicated to interpret… it is extremely difficult to express in the abstract a set of performance characteristics for a system intended to screen the universe of all possible sequences."	[65]	G, U
	Increased capacity for generating enormous, diverse pools of oligo-length sequences and lower-cost methods for assembling high-quality, gene-length sequences from oligo pools "create a potential vulnerability: what would be considered controlled for genelength synthesis under current regulatory and technical systems would be permitted for synthesis as an oligo pool and could be converted into a gene length sequence by assembly in a modestly equipped molecular biology laboratory."	ibid.	G
	Concern for "venue shopping:" "a bad actor intent on acquiring dangerous sequences could submit an order to multiple companies in the hope of finding a company whose screening system will permit the order."	ibid.	G
	"biofoundries may unwittingly produce components of high consequence biological agents solely from digital information provided by the customer."	[5]	CP,G
	"While resequencing could be used to identify and correct sequence errors, it is only possible when the original source material is available."	[37]	C,G
Advanced manufacturing/evolving platforms	"The production processes and assemblies of biologics and other materials can also be distributed and carried out asynchronously at geographically different locations..."	[38]	G, U
	"Virtual environments allow access to infrastructure within the physical world; this creates a vulnerability that would permit unauthorized remote access to an automated biological manufacturing system."	ibid.	CP
	"Attackers may cause sensors to report false data or modify algorithms in control systems in ways that can jeopardize product quality, damage manufacturing equipment, and potentially induce occupational hazards."	[22]	CP
	Regarding "smart labs" of the future: "adjustment of fan speeds in building ventilation systems… can lead to potential exposure of any building occupant to infectious microorganisms or their toxic products, contamination of the facility, or airborne release of pathogens to the surrounding external environment… changes to chemical concentration and/or holding time in liquid effluent decontamination systems which can result in premature discharge of infectious, toxic byproducts or genetically altered microorganisms to the municipal waste stream."	[20]	CP
	"To obscure the identity and/or functional properties of the final product several biofoundries can be used, each synthesizing seemingly innocuous products representing only a portion of the final product."	[5]	G, U
Food, agriculture, water	"The health and security… of agriculture and food systems is unclear from a cyberbiosecurity perspective. We reason that vulnerable critical links and nodes exist throughout this highly complex global and national ecosystem."	[38]	V

Table 1 (*continued*)

Area of biorisk concern	Description of dangers/consequences[a]	Source	Major attack potential[b]
	"A recent contamination event of an unauthorized GM *Bacillus subtilis* strain (Paracchini et al., 2017) in Europe could have been - or the same way could be - the consequence of exploiting gaps of prevailing DNA signatures." "DNA signatures may intentionally be exploited to support the counterfeiting or even weaponization of GM organisms."	[14]	CP,G
	"The identification and analysis of harmful genetic manipulations to utilize (covertly modified) plants (GMOs and non-GMOs) as an attack vector show that these concerns need to be taken seriously, raising the prospect not only of direct harm, but of the more likely effects in generating public concern, reputational harm of agricultural biotechnology companies, law-suits, and increased import bans of certain plants or their derived products."	[39]	CP,G,U
	Water security exemplified via harmful algal blooms (HAB): "it is imperative to envision water security from the perspective of a cyber-physical system (CPS)." Attacks on HAB-monitoring systems include "data injection attacks, automated system hijacking attacks, node forgery attacks, and attacks on learning algorithms."	[67]	CP

[a] For the citations within quotations, please see the citing literature for details.

[b] C-cyber, CP-cyberphysical, G-gap between digital and physical description/entity/process (Section 5.2), V-various, U-unique concerns (e.g., due to 'biologic information,' Section 4.1; see also [39]).

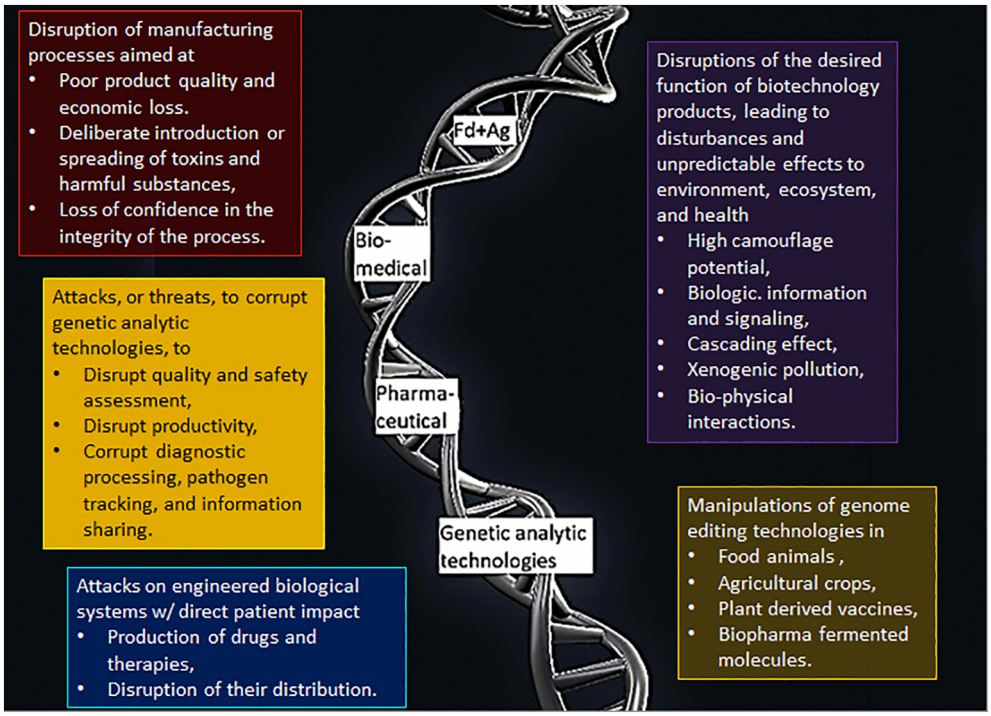

Fig. 2. Examples of cyberbio risks. Most of these have only recently been identified and could jeopardize numerous branches of the bioeconomy, including critical manufacturing, food and agriculture, healthcare and public health.

– Weak or non-existent deterrent and enforcement measures and the lack of standards and guidelines [11,21,33] are serious issues to achieve comprehensive and international protection.

4. Pressing and unique dangers and consequences

Very recent publications and programs [7,32,40–46]) undoubtedly have increased cyberbiosecurity awareness, and large corporations will have been able to enhance their infrastructure. The 2020 pandemic has shifted R&D priorities and budget and has hampered many efforts to better comprehend the new risks and develop solutions. Pharma and MedTech professionals and companies are overwhelmed with COVID-19 mitigation and crisis resolution while the industry sprints to develop new therapeutics and vaccines. On the other hand, the pandemic has led to a massive rise in cyber-attacks, with some reporting an 800% increase compared to pre-coronavirus levels [47]. As cybersecurity professionals are struggling to target this surge in cyber-crime, WFH (work from home) has impacted many cybersecurity professionals' ability to support new business applications or initiatives [48]. As companies and organizations struggle to maintain stability and security, new research areas such as cyberbiosecurity have received inadequate attention and support.

In addition to the known cyberbio challenges described above, the context of the bioscience fields leads to distinct problems that are not well understood.

4.1. High impact consequences in the life-science context

The context of the life-sciences involves unique concerns and unknowns. Cyber-based attacks targeting the biological and medical sciences involve living entities with networks of connections, combinatorial interactions, and a dynamic range of outcomes. Future and timed effects can be achieved by various technologies (e.g., non-volatile memory devices and electronic circuits). Nevertheless, with biotechnology products there is a decreased ability to control exposure [49]. They are often designed to be

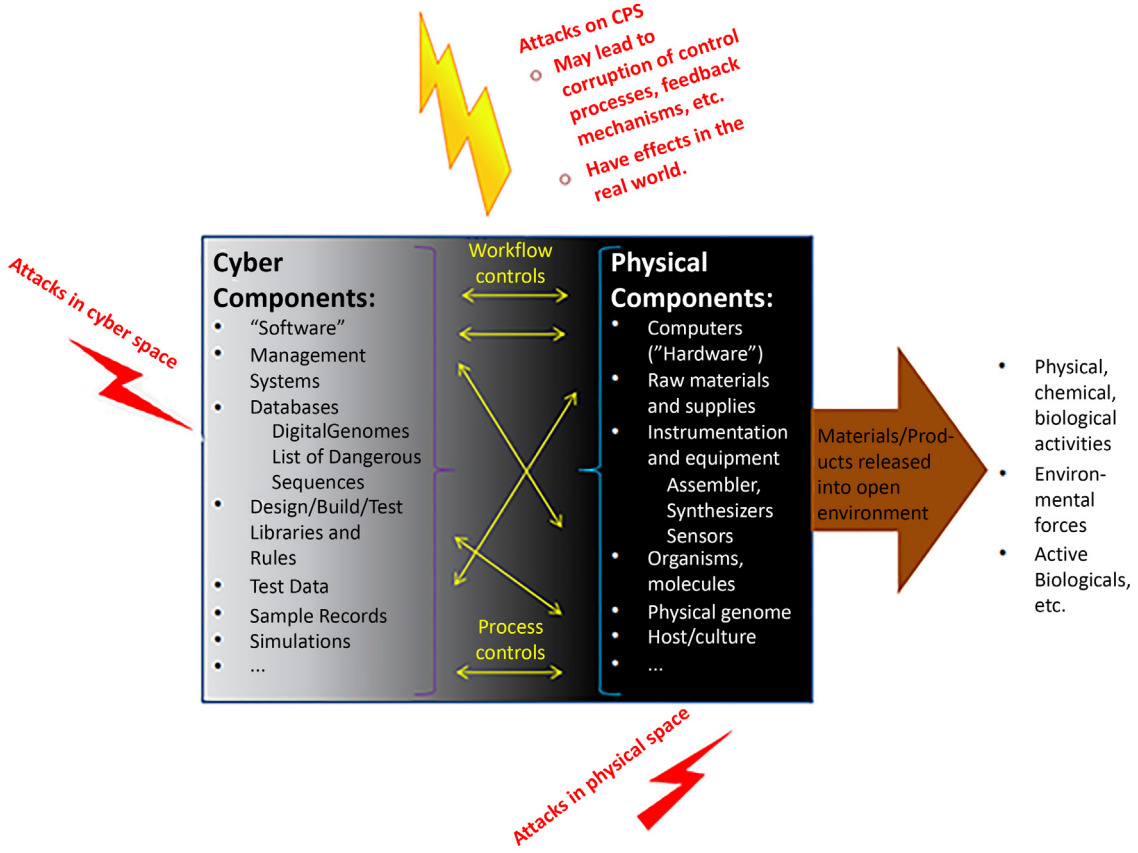

Fig. 3. CPS and their security in the biological sciences. The reliance on CPS may enable unanticipated security risks and threats (lightning bolts). In addition to the engineered framework of a CPS (central box), impacts and consequences across the life-science fields also need to be considered in the open environment (right arrow, see Section 4.1).

easily dispersed (e.g., with agricultural technologies directly in the field [50]), reach high scalability [49], can be delivered in different states (including water [51]), and can be activated by simple environmental agents (temperature, light, wind [52–54]).

A critical issue with active biologicals is that they can be transferred by contact, ingestion, or inhalation [49]. While concerns about unintended consequences and ill-intended applications of these and related technologies have been raised recently (see e.g., [7,13,17,32,49,55,56]), types of biotechnologies that not merely have a cyber-overlap, but which constitute artificial systems themselves, have been even less assessed. These include artificially generated self-replicating systems [57], artificial cells that mimic the ability of natural cells to communicate with bacteria [58], or artificially generated processes to interact with one another and initiate various signaling cascades [59]. The consequences of an ill-intended or accidental release of such systems into the environment are not understood.

One of the most complex issues may be that 'information' in the biological context is of a different kind than what is meant in the information sciences. Identifying 'biological information' is not always straightforward and may evade available technology from time to time: consider, for instance, the situation of recessive alleles of a gene. These can be phenotypically invisible over a huge proportion of a population and known for their frequency using tools such as the Hardy Weinberg equilibrium equation; as DNA sequencing and synthesizing technologies developed over decades, they could be detected and linked to individuals. While such invisibility features are of potential benefit in steganography, [60] describes critical concerns that analogously apply to cyberbiosecurity. For instance, biological information can be stored and transmitted in a virtually undetectable way: "No X-ray, infra-red scanner, chemical assay or body search will provide any immediate evidence" of it [60]. Further, biological media can survive much longer than anticipated [50], which in this context leads to the worrisome situation that data (or biologic 'information') can "literally run off on its own" [60].

Notably, critical vulnerabilities also arise in the context of devices and mechanisms. Among others, the survey mentioned above [8] identified "elevated or severe risk" potentials for an unauthorized actor to (1) take control of infrastructure (e.g., lab equipment, lab control systems, or even a fully automated robot lab), (2) interrupt the functioning of lab systems, or (3) circumventing security controls. The cyber-physical nature of biotechnology is one of the key concerns in cyberbiosecurity (Fig. 3 and Table 1). With increased automation, dangers arise, for example, in the context of sterilization methods used in the healthcare and laboratory setting. For some methods, a very recent study [61] demonstrates that "integrity of released DNA is not completely compromised," which is leading to the "danger of dissemination of DNA and xenogenic elements across waterways." These findings were linked to temperature and time (e.g., short microwave exposure times or short exposure time to glutaraldehyde treatment were least effective). Parameters like these are both highly malleable and susceptible to manipulation, which will become an even more significant concern with "smart labs" of the future [20]. In the context of food and agricultural systems, cyberphysical interconnections lead to the danger of "Manipulation of critical automated (computer-based) processes (e.g., thermal processing time and temperature for food safety)" and "Lack of ability to perform vulnerability assessment" [33].

4.2. Security psychology and the human factor in the life-science fields

Traditionally, the reliance on tacit knowledge and direct hands-on processes and applications has shielded the bioscience field from many forms of attack. Beyond doubt, the digitization of biology and biotechnology automation are key drivers that enable the bioeconomy. Nonetheless, these are

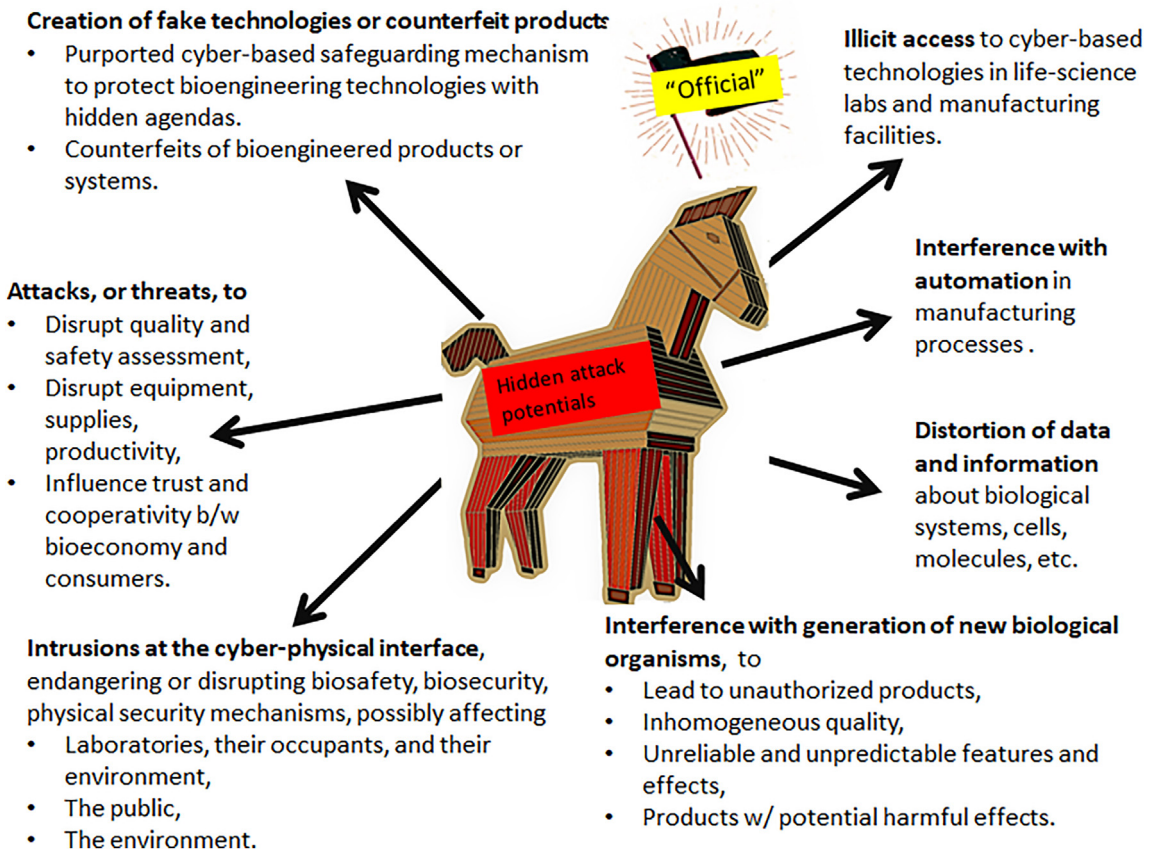

Fig. 4. Attacks targeting the life-science fields that are based on psychology. The Trojan horse depicts cyber-enabled attack potentials, based on officially looking hoaxes and frauds (Table 2) or subvertable safeguarding mechanisms.

creating yet a different type of risk than described above. The Internet makes it easier to bypass our existing controls (personal intuitions, company procedures or even laws) [62]. We have evolved social and psychological tools over millions of years to help us deal with deception in face-to-face contexts. However,when we lose both physical and human context (as in online communication), forgery and intrusion become more of a risk.

It is now known that in the cyber fields "Deception, of various kinds, is now the principal mechanism used to defeat online security" [62]. Online frauds are often easier to do, but harder to stop than similar real-world frauds. Furthermore, according to [63], "more and more crimes involve deception; as security engineering gets better, it's easier to mislead people than to hack computers or hack through walls."

While only recently recognized as one of the most important components of security engineering [62], the entire life-science enterprise is not adequately prepared for attacks that exploit psychology (social engineering attacks, Table 2).

At the same time, hackers are getting better at technology: "designers learn how to forestall the easier technical attacks..." [62]. Thus, through various forms of fraud and deception, attackers may be able to circumvent many of the existing cyber-based safeguarding mechanisms and get direct access to their victim's system. Once they have entry to a target system, this may allow them to exploit not only the data and cyber side; it could also facilitate attacks on control and processes underlying various cyber-physical applications (Fig. 3). The consequences will directly affect biophysical components (Fig. 4).

4.3. Real attacks, or just hoax

In addition to actual exploitations, often the mere threat of attacks alone could have drastic consequences. Think about a situation, for instance, where attackers claim to secretly have gained access to some of the underlying (cyber-based) routines, that they have created a new and highly pathogenic and infectious virus, or that they have introduced manipulated counterfeit products (including foods, feed, drugs) into the supply chain. In addition to creating public fear, hoax, failed attacks, or attacks staged with benign biologicals can also help attackers to test responses and look for patterns that reveal other vulnerabilities. This is known in the context of GMOs where the testing capability of a country that limits GMO levels can be determined by contaminating shipments with known levels of GM ingredients [64].

5. Recommendations

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. As cyberbiosecurity may profit the most from lessons learned in the information security domains, this section focuses on this arena.

5.1. Identifying the potentials of existing cyber approaches

Several suggestions have been made to secure specific new cyberbio challenges via various cyber applications (e.g. [5,10,12,14,20,37,65]). Nonetheless, their practical realization is not always straightforward as even most basic information security notions still need to be better adapted to the bioscience framework (see e.g. [14, Table 1]). Similarly, it will be necessary to refine and extend the classic CIA triad (which long has been the heart of information security), to extend the

suggestions made previously (e.g. [14, Fig. 3]), to optimally align them with the new demands.

5.2. Recognizing and hierarchizing new challenges

As argued (Section 4.1), not all the new problems can be linked to traditional cyber issues. Thus, it will be essential to distinguish which challenges could, or could not, be identified/safeguarded by existing cyber-approaches (or slight modifications thereof). To aid this distinction and develop a hierarchy of risk severity, it will help to pinpoint the following.

5.3. Identify challenges to assure authenticity and integrity

The cyber-based interface to measure and assess a bioengineered product or service creates a gap, potentially allowing a range of vulnerabilities from falsifiable entries of biological databases and sequence errors [12,37] - which in a context like pathogens could lead to entry errors with rather disturbing effects - the intentional tampering of data related to forensics [66], cyber- enabled attacks on systems monitoring water security [67], to the actual exchange of the purported actual (CPS produced) entity. The latter may enable the distribution of accidentally exchanged/counterfeit products such as plasmids [19] or illicit feed additives and contaminated feed consignments [39,68,69]. Such a gap may be exploited by attackers to hide manipulated (hazardous) biologicals behind the digital description of its natural or (when engineered), legitimate and approved counterparts.

5.3.1. Distinguish products and services that do not resemble a 'closed box'

Quality tests need to be reconsidered as the actual, final system or product may resemble a different entity than reported by its (digitized) description. For instance, with modern engineering techniques, attackers may be able to surreptitiously insert modifications into different loci of the genome and create alterations leading to changes in gene expression [39], or assemble high-consequence, gene-length sequences out of seemingly innocuous components [65]. Although I first considered this dilemma almost a decade ago [15] (see also [16,70]), modern gene-editing techniques give rise to unprecedented challenges. While in [14] I suggested basics for some new approaches, more work needs to be done for practical and efficient realizations. Another serious problem arises in the context of labeling, particularly when something else can change the content later. This is the case with active biologicals (Section 4.1) which give rise to unique concerns when, e.g. some undeclared and 'invisible' protein or nucleic acid in a suspended formulation contacts the stated product on release from the packaging or in the retail chain (see [49]).

5.3.2. Identify the possibility of biologic information to 'run off,' and potentially lead to unintended consequences

Control and quality assurance measurements can only reveal the present and past (but not future) conditions of a biological (i.e., dynamic) system and yield an incomplete basis for traditional cyber protection. Safeguarding policies should therefore consider unique features of 'information' in the biological sciences [60], the information life-cycle at large, logically-based game strategies, mechanisms for dual-use appropriation, end-to-end assessments, 'routes to harm,' context, and multiple exposure pathways [10,13,34,39,49,56,65].

5.3.3. Identify the possibility of future and off-target effects

These are situations where precise predictions as required for various 'if-then' paradigms employed in the cyber domains are inapplicable. Deterrence measures will need to consider emerging actors and their pathways of action, including interactions between synthetic and natural entities, as well as mechanisms, vesicles and actions that can be activated by various physical and mechanical forces or combinations thereof [49,67].

Table 2
Social engineering hacks.

Social engineering in the cyber-domain	Social engineering targeting the bioscience fields
Pretexts are some of the quickest ways of getting past a company's switchboard and winning its people's trust. • E.g., via a fake email from a purported colleague who offers 'help' with resetting your password, or the security department of your bank alerting you about suspicious activities in your account. • Pretexting is the basis of social security attacks - in this context "the intentional manipulation of people into performing certain actions and divulging confidential information" [72].	On the pretext of helping to safeguard cyberbiosecurity challenges, attackers could • Offer a solution to the new cyberbio challenges - which are mainly un-assessed and for which no adequate official solutions exist. • Masquerade it as an officially-looking tool and written in a language that is comprehensible to those interested in applying it. • Secretly introduce harmful computer code that could enable theft of sensitive information or access to critical CPS based infrastructure components.
Many devastating IT hacks are based on mere deception [62], e.g. • Fake websites and phishing scams are trying to lure their victims into buying high-demand products such as masks, hand sanitizers or vitamins. • They may be riddled behind the scenes with malware, (computer) viruses, and ransomware.	The entire life-science field is particularly vulnerable to such psychological hacks promoting fake products: • There is a great demand for products and services such as research and bioinformatics tools or various model systems. • Phishing scams may appear to come from official organizations such as the CDC (Centers for Disease Control) or the WHO (World Health Organization); fake webites may masquerade as authentic R&D data providers including preprint servers; newly developed websites registered with catch-phrases such as 'corona' may be legitimate sources of information. • All these may have been maliciously designed to carry out spam campaigns, phishing, or to spread harmful software.
Fake internal contacts (mostly by email): • Fake HR or IT contacts are often used to steal usernames and passwords. • The impersonation of HR or IT departments often allows attackers to gain access to sensitive data and information.	If attackers canimpersonate HR or IT departments, this could allow them to • Steal secret R&D data and information. • Enter the target system to upload malicious cyber programs that could be used to sabotage the physical processes underlying biotechnological systems (Section 2). • Use stolen credentials to impersonate another user in that network to enable the corruption of environmentally or health-related processes, sensors, or data.
Cyberattacks are not always 100% committed online. Social engineering schemes can allow attackers to hack into large businesses or organizations (exemplified here via the July 2020 Twitter attack [72]). • The hacker was able to take control of a cell phone number by convincing a carrier to assign a number to a new phone. • The attacker hacked into Twitter accounts of famous people and organizations. For some of the hacked accounts, the attacker could initiate a password reset, login to the account, and send Tweets [72]. • The attacker was able to view personal information including email addresses and phone numbers, which are displayed to some users of Twitter's internal support tools [72].	Businesses and CPS networks throughout the bioscience fields are susceptible to analogous attacks via fake phone or email contacts, e.g. • Attackers could mislead certain employees and exploit human vulnerabilities to hack into the accounts of some employees. • By using the credentials of only a few hacked employees, attackers may be able to access the internal computer system. • This knowledge may enable them to target additional employees with access to system management tools. • These credentials can give them access to internal network tools and enable them to sabotage cyber-based controls of CPS (Figs. 3 and 4).

5.4. CPS

Cyberbio efforts will benefit from the CPS arena as these provide unique insights relative to 'hardware' (incl. devices and systems) and

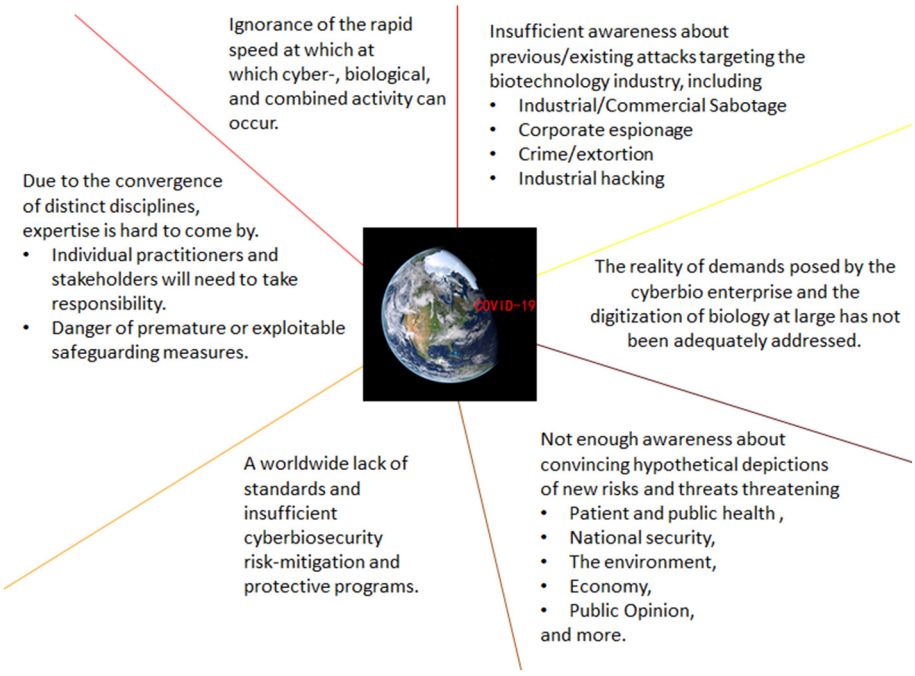

Fig. 5. State of the art of cyberbiosecurity. While the entire globe is trying to explain the origins of SARS-CoV-2 and is busy with COVID-19 mitigation and crisis resolution, the situation regarding cyberbiosecurity is sobering.

'software' interdependencies. The cyber-interactions and the interconnectedness of such systems necessitate a drastic modification of previous security principles (see e.g., [28,71]). Analogously, for cyberbio systems and mechanisms, it will be necessary to refine a list of security principles and goals, by incorporating CPS lessons, to optimally align them with the bioscience fields.

6. Conclusion

Cyberbiosecurity is an evolving paradigm that points to new gaps and risks, fostered by modern biotechnologies' cyber-overlaps. The enormous increase in computational capabilities, artificial intelligence, automation, and engineering principles in the bioscience field have created a realm with a glaring gap of adequate controls. Vulnerabilities exist within biomanufacturing, cyber-enabled laboratory instrumentation and patient-focused systems, "Big Data" generated from "omics" studies, and throughout the farm-to-table enterprise…" [38]. Numerous security risks in the biological sciences and attack potentials based on psychology have not been adequately assessed, let alone captured. They will require entirely new approaches towards their protection to avoid emergencies at the scale of COVID-19 or more. Yet, the current situation regarding cyberbiosecurity is sobering (Fig. 5). The private sector, small and moderate-sized companies, and the broader DIY community itself are particularly vulnerable [7,11,33]. Rather than spending enormous amounts of resources in looking back to identify the exact genesis of SARS-CoV-2, cause of the pandemic, and the emphasized indentity of our current global situation, a concerted effort to better understand and mitigate the emerging cyberbio challenges faced by the entire bioeconomy sector should be a top priority. This paper summarizes existing critical issues that must be considered. It also suggests steps that can be leveraged to help assess and ensure that the many bioscience capabilities remain dependable in the face of malice, error, or mischance.

Conflict of interest statement

The author declares that there are no conflicts of interest.

References

[1] Food and Agriculture Organization of the United Nations, Report on the exploratory fact-finding scoping study on "digital sequence information" on genetic resources for food and agriculture. http://www.fao.org/3/CA2359EN/ca2359en.pdf, 2018 (accessed 20 April 2020).
[2] Third World Network, Comments of third world network on digital sequence information. https://www.cbd.int/abs/DSI-views/2019/TWN-DSI.pdf, 2019 (accessed 20 April 2020).
[3] R. Murch, D. DiEuliis, Editorial: mapping the cyberbiosecurity enterprise, Front. Bioeng. Biotechnol. 7 (2019) 235, https://doi.org/10.3389/fbioe.2019.00235.
[4] R.S. Murch, W.K. So, W.G. Buchholz, S. Raman, J. Peccoud, Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy, Front. Bioeng. Biotechnol. 6 (2018) 39, https://doi.org/10.3389/fbioe.2018.00039.
[5] D.S. Schabacker, L.-A. Levy, N.J. Evans, J.M. Fowler, E.A. Dickey, Assessing cyberbiosecurity vulnerabilities and infrastructure resilience, Front. Bioeng. Biotechnol. 7 (2019) 61, https://doi.org/10.3389/fbioe.2019.00061.
[6] P. Ney, K. Koscher, L. Organick, L. Ceze, T. Kohno, Computer security, privacy, and DNA sequencing: compromising computers with synthesized DNA, privacy leaks, and more, 26th USENIX Security Symposium (USENIX Security 17), USENIX Association, Vancouver, BC 2017, pp. 765–779.
[7] National Academies of Sciences, Engineering, and Medicine, Safeguarding the bioeconomy, The National Academies Press, Washington, DC, 2020. https://doi.org/10.17226/25525.
[8] K. Millett, E. dos Santos, P.D. Millett, Cyber-biosecurity risk perceptions in the biotech sector, Front. Bioeng. Biotechnol. 7 (2019) 136, https://doi.org/10.3389/fbioe.2019.00136.
[9] B. Knapp, Fifith Domamin, Researchers are sounding the alarm on cyberbiosecurity. https://www.fifthdomain.com/dod/2018/02/08/researchers-are-sounding-the-alarm-on-cyberbiosecurity/, 2018 (accessed 20 April 2020).
[10] K.M. Berger, P.A. Schneck, National and transnational security implications of asymmetric access to and use of biological data, Front. Bioeng. Biotechnol. 7 (2019) 21, https://doi.org/10.3389/fbioe.2019.00021.
[11] A.M. George, The national security implications of cyberbiosecurity, Front. Bioeng. Biotechnol. 7 (2019) 51, https://doi.org/10.3389/fbioe.2019.00051.
[12] B.A. Vinatzer, L.S. Heath, H.M.J. Almohri, M.J. Stulberg, C. Lowe, S. Li, Cyberbiosecurity challenges of pathogen genome databases, Front. Bioeng. Biotechnol. 7 (2019) 106, https://doi.org/10.3389/fbioe.2019.00106.
[13] N. Bajema, D. DiEuliis, C. Lutes, Y. Lim, The digitization of biology: understanding the new risks and implications for governance, Tech. rep, National Defense University, Center for the Study of Weapons of Mass Destruction. https://www.hsdl.org/?view&did=813127, 2018 (accessed 20 April 2020).
[14] S. Mueller, On DNA signatures, their dual-use potential for GMO counterfeiting, and a cyber-based security solution, Front. Bioeng. Biotechnol. 7 (2019) 189–197, https://doi.org/10.3389/fbioe.2019.00189.

[15] S. Mueller, The DNA code: Implications for efficiency and security, dissertation, University of Wyoming, 2014.
[16] S. Mueller, F. Jafari, D. Roth, A covert authentication and security solution for GMOs, BMC Bioinformatics 17 (2016) 389, https://doi.org/10.1186/s12859-016-1256-6.
[17] B.C. Wintle, C.R. Boehm, C. Rhodes, J.C. Molloy, P. Millett, L. Adam, R. Breitling, R. Carlson, R. Casagrande, M. Dando, et al., Point of view: a transatlantic perspective on 20 emerging issues in biological engineering, Elife 6 (2017), e30247. https://doi.org/10.7554/eLife.30247.
[18] G. Dunlap, E. Pauwels, The intelligent and connected bio-labs of the future. https://www.wilsoncenter.org/sites/default/files/media/documents/misc/the_intelligent_connected_biolabs_of_the_future.pdf, 2017 (accessed 20 April 2020).
[19] J. Peccoud, J.E. Gallegos, R. Murch, W.G. Buchholz, S. Raman, Cyberbiosecurity: from naive trust to risk awareness, Trends Biotechnol. 36 (1) (2018) 4–7, https://doi.org/10.1016/j.tibtech.2017.10.012.
[20] J.C. Reed, N. Dunaway, Cyberbiosecurity implications for the laboratory of the future, Front. Bioeng. Biotechnol. 7 (2019) 182, https://doi.org/10.3389/fbioe.2019.00182.
[21] L.C. Richardson, S.M. Lewis, R.N. Burnette, Building capacity for cyberbiosecurity training, Front. Bioeng. Biotechnol. 7 (2019) 112, https://doi.org/10.3389/fbioe.2019.00112.
[22] D. Guttieres, S. Stewart, J. Wolfrum, S.L. Springs, Cyberbiosecurity in advanced manufacturing models, Front. Bioeng. Biotechnol. 7 (2019) 210, https://doi.org/10.3389/fbioe.2019.00210.
[23] J. Sackner-Bernstein, Design of hack-resistant diabetes devices and disclosure of their cyber safety, J. Diabetes Sci. Technol. 11 (2) (2017) 198–202, https://doi.org/10.1177/1932296816678264.
[24] BBC News Services, US hospitals turn away patients as ransomware strikes. https://www.bbc.com/news/technology-49905226, 2019 (accessed 20 April 2020).
[25] R. Gallagher, Bloomberg, Hackers 'without conscience' demand ransom from dozens of hospitals and labs working on coronavirus. https://www.bloomberg.com/news/articles/2020-04-01/hackers-without-conscience-demand-ransom-from-health-providers, 2020 (accessed 20 April 2020).
[26] C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monticone, Cybersecurity in healthcare: a systematic review of modern threats and trends, Technol. Health Care 25 (1) (2017) 1–10, https://doi.org/10.3233/THC-161263.
[27] Institute for Critical Infrastructure Technology, The cybersecurity think tank. https://icitech.org/, 2020 (accessed 20 April 2020).
[28] G.A. Fink, T.W. Edgar, T.R. Rice, D.G. MacDonald, C.E. Crawford, Overview of security and privacy in cyber-physical systems, security and privacy in cyber-physical systems: foundations, Principles Appl. (2017) 1–23, https://doi.org/10.1002/9781119226079.ch1.
[29] J. Robertson, M. Riley, Mysterious 08 turkey pipeline blast opened new cyberwar era. https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar, 2014 (accessed 20 April 2020).
[30] Tu Wien Informatics, Cyber-Physical System Group. https://ti.tuwien.ac.at/cps, 2020 (accessd 20 April 2020).
[31] K.I. Berns, A. Casadevall, M.L. Cohen, S.A. Ehrlich, L.W. Enquist, J.P. Fitch, D.R. Franz, C.M. Fraser-Liggett, C.M. Grant, M.J. Imperiale, et al., Adaptations of avian flu virus are a cause for concern, Science 335 (6069) (2012) 660–661, https://doi.org/10.1126/science.1217994.
[32] Frontiers Research Topic, Mapping the cyberbiosecurity enterprise. https://www.frontiersin.org/research-topics/8353/mapping-the-cyberbiosecurity-enterprise, 2019 (accessed 20 April 2020).
[33] S.E. Duncan, R. Reinhard, R.C. Williams, F. Ramsey, W. Thomason, K. Lee, N. Dudek, S. Mostaghimi, E. Colbert, R. Murch, Cyberbiosecurity: a new perspective on protecting U.S. food and agricultural system, Front. Bioeng. Biotechnol. 7 (2019) 63, https://doi.org/10.3389/fbioe.2019.00063.
[34] J.L. Mantle, J. Rammohan, E.F. Romantseva, J.T. Welch, L.R. Kauffman, J. McCarthy, J. Schiel, J.C. Baker, E.A. Strychalski, K.C. Rogers, K.H. Lee, Cyberbiosecurity for biopharmaceutical products, Front. Bioeng. Biotechnol. 7 (2019) 116, https://doi.org/10.3389/fbioe.2019.00116.
[35] Department of Homeland Security, Infrastructure Survey Tool. https://www.dhs.gov/cisa/infrastructure-survey-tool (accessed 20 April 2020).
[36] National Institute of Standards and Technology, Cybersecurity framework. https://www.treasury.gov/initiatives/fio/Documents/NIST%20Framework%20Core%20Sheet_20140515%20(2).pdf, 2018 (accessed 20 April 2020).
[37] J. Caswell, J.D. Gans, N. Generous, C.M. Hudson, E. Merkley, C. Johnson, C. Oehmen, K. Omberg, E. Purvine, K. Taylor, C.L. Ting, M. Wolinsky, G. Xie, Defending our public biological databases as a global critical infrastructure, Front. Bioeng. Biotechnol. 7 (2019) 58, https://doi.org/10.3389/fbioe.2019.00058.
[38] L.C. Richardson, N.D. Connell, S.M. Lewis, E. Pauwels, R.S. Murch, Cyberbiosecurity: a call for cooperation in a new threat landscape, Front. Bioeng. Biotechnol. 7 (2019) 99, https://doi.org/10.3389/fbioe.2019.00099.
[39] S. Mueller, Are market GM plants an unrecognized platform for bioterrorism and biocrime? Front. Bioeng. Biotechnol. 7 (2019) 121, https://doi.org/10.3389/fbioe.2019.00121.
[40] U.S. Department of Health & Human Services, Department of health and human services framework for guiding funding decisions about proposed research involving enhanced potential pandemic pathogens, The S3: Science, Safety, Security Project. https://www.phe.gov/s3/dualuse/Pages/p3co.aspx, 2017 (accessed 20 April 2020)
[41] The Australia Group, The Australia Group. https://australiagroup.net/en/index.html (accessed 20 April 2020).
[42] The Nuclear Threat Initiative, Biosecurity reducing biological risk and enhancing global biosecurity. https://www.nti.org/about/biosecurity/ (accessed 20 April 2020).
[43] Global Health Security Initiative. http://ghsi.ca/, 2001 (accessed 20 April 2020).
[44] OECD, Vbc launches biosecurity codes section. https://www.virtualbiosecuritycenter.org/blog/post_tag/oecd/ 2011 (accessed April 2020).
[45] National Institutes of Health, National Science Advisory Board for Biosecurity. https://osp.od.nih.gov/biotechnology/national-science-advisory-board-for-biosecurity-nsabb/ (accessed 20 April 2020).
[46] Bipartisan Commission on Biodefense, Blue ribbon study panel on biodefense. https://biodefensecommission.org/, 2020 (accessed 20 April 2020).
[47] CISION PR Newswire, Top cyber security experts report: 4,000 cyber attacks a day since Covid-19 pandemic. https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html, 2020 (accessed 20 April 2020).
[48] Help Net Security, The Covid-19 pandemic and its impact on cybersecurity. https://www.helpnetsecurity.com/2020/08/03/pandemic-impact-cybersecurity/, 2020 (accessed 15 August 2020).
[49] J.A. Heinemann, S. Walker, Environmentally applied nucleic acids and proteins for purposes of engineering changes to genes and other genetic material, Biosaf. Health 1 (3) (2019) 113–123, https://doi.org/10.1016/j.bsheal.2019.09.003.
[50] R. Reeves, S. Voeneky, D. Caetano-Anollés, F. Beck, C. Boëte, Agricultural research, or a new bioweapon system? Science 362 (6410) (2018) 35–37, https://doi.org/10.1126/science.aat7664.
[51] N. Mitter, Z.P. Xu, G.Q. Lu, Plant-protecting RNAi compositions comprising plant-protecting double-stranded RNA adsorbed onto layered double hydroxide particles. https://patents.google.com/patent/US20170029819A1/en, 2015 (accessed 20 April 2020).
[52] G. P. Drouillard, Systems and methods for delivering nucleic acids to a plant, US Patent and Trademark Office. http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=17&f=G&l=50&d=PG01&S1=Drouillard&OS=Drouillard&RS=Drouillard, 2019 (accessed 20 April 2020).
[53] S. Huang, A. B. Iandolino, G. J. Peel, Methods and compositions for introducing nucleic acids into plants, US Patent and Trademark Office. http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&f=G&l=50&d=PG01&p=1&S1=Landolino&OS=Landolino&RS=Landolino, 2018 (accessed 20 April 2020).
[54] K. San Miguel, J.G. Scott, The next generation of insecticides: dsRNA is stable as a foliar-applied insecticide, Pest Manag. Sci. 72 (4) (2016) 801–809, https://doi.org/10.1002/ps.4056.
[55] M. Bizzarri, The New Alchemists: The Risks of Genetic Modification, The New Alchemists: The Risks of Genetic Modification, WIT Press, 2012.
[56] D. DiEuliis, J. Giordano, Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons, Health Secur. 15 (3) (2017) 296–302, https://doi.org/10.1089/hs.2016.0120.
[57] V. Noireaux, Y.T. Maeda, A. Libchaber, Development of an artificial cell, from self-organization to computation and self-reproduction, Proc. Natl. Acad. Sci. 108 (9) (2011) 3473–3480, https://doi.org/10.1073/pnas.1017075108.
[58] R. Lentini, N.Y. Martín, M. Forlin, L. Belmonte, J. Fontana, M. Cornella, L. Martini, S. Tamburini, W.E. Bentley, O. Jousson, et al., Two-way chemical communication between artificial and natural cells, ACS Central Sci. 3 (2) (2017) 117–123, https://doi.org/10.1021/acscentsci.6b00330.
[59] Y. Elani, R.V. Law, O. Ces, Vesicle-based artificial cells as chemical microreactors with spatially segregated reaction pathways, Nat. Commun. 5 (2014) 5305, https://doi.org/10.1038/ncomms6305.
[60] T.D. Brunet, Aims and methods of biosteganography, J. Biotechnol. 226 (2016) 56–64, https://doi.org/10.1016/j.jbiotec.2016.03.044.
[61] D. Calderón-Franco, Q. Lin, M. van Loosdrecht, B. Abbas, D.G. Weissbrodt, Anticipating xenogenic pollution at the source: impact of sterilizations on DNA release from microbial cultures, Front. Bioeng. Biotechnol. 8 (2020) 171, https://doi.org/10.3389/fbioe.2020.00171.
[62] R. Anderson, Security Engineering, Third edition Wiley, New Jersey, 2020.
[63] R. Anderson, Psychology and Security Resource Page. https://www.cl.cam.ac.uk/~rja14/psysec.html, 2019 (accessed 20 April 2020).
[64] J.A. Heinemann, A.D. Sparrow, T. Traavik, Is confidence in the monitoring of ge foods justified? Trends Biotechnol. 22 (7) (2004) 331–336, https://doi.org/10.1016/j.tibtech.2004.05.002.
[65] J. Diggans, E. Leproust, Next steps for access to safe, secure DNA synthesis, Front. Bioeng. Biotechnol. 7 (2019) 86, https://doi.org/10.3389/fbioe.2019.00086.
[66] E.A. Franzosa, K. Huang, J.F. Meadow, D. Gevers, K.P. Lemon, B.J. Bohannan, C. Huttenhower, Identifying personal microbiomes using metagenomic codes, Proc. Natl. Acad. Sci. 112 (22) (2015), E2930–E2938. https://doi.org/10.1073/pnas.1423854112.
[67] D.G. Schmale III, A.P. Ault, W. Saad, D.T. Scott, J.A. Westrick, Perspectives on harmful algal blooms (HABs) and the cyberbiosecurity of freshwater systems, Front. Bioeng. Biotechnol. 7 (2019) 128, https://doi.org/10.3389/fbioe.2019.00128.
[68] V. Paracchini, M. Petrillo, R. Reiting, A. Angers-Loustau, D. Wahler, A. Stolz, B. Schönig, A. Matthies, J. Bendiek, D.M. Meinel, S. Pecoraro, U. Busch, A. Patak, J. Kreysa, L. Grohmann, Molecular characterization of an unauthorized genetically modified bacillus subtilis production strain identified in a vitamin b 2 feed additive, Food Chem. 230 (2017) 681–689, https://doi.org/10.1016/j.foodchem.2017.03.042.
[69] N. Rostoks, L. Grantiņa-Ieviņa, B. Ieviņa, V. Evelone, O. Valciņa, I. Aleksejeva, Genetically modified seeds and plant propagating material in europe: potential routes of

entrance and current status, Heliyon 5 (2) (2019), e01242. https://doi.org/10.1016/j.heliyon.2019.e01242.
[70] D. Roth, S. Mueller, F. Jafari, Methods for data encoding in DNA and genetically modified organism authentication, united States Patent, Pub. No.: US 2019/0089372 A1, 2019.
[71] Y. Cherdantseva, J. Hilton, A reference model of information assurance & security, 2013 International Conference on Availability, Reliability and Security, IEEE (2013) 546–555, https://doi.org/10.1109/ARES.2013.72.
[72] Twitter Inc., An Update on Our Security Incident. https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html, 2020 (accessed 15 August 2020).