Cyber-Biosecurity; a Paradigm Shift In the Field Of Life Sciences And Agriculture Sector

Abstract:

The fields of information technology (IT) and cybersecurity are becoming more integrated with the life sciences. This convergence is a fundamental driver in the boom of biotechnology research and its industrial applications in health care, agriculture, manufacturing, automation, artificial intelligence, and synthetic biology. Other drivers include artificial intelligence and genetic engineering. Many market sectors are now susceptible to dangers posed by the digital interface as a result of the rising digitization of information and the handling mechanisms for biological materials. Cyber-biosecurity, a new topic developing at the intersection of the biological sciences and the information technology fields, will be developed to handle this expanding scenario. Life sciences frequently merge with information technology and cyber-security in the new digital era. With the advancements in biomedical research and the scientific advancement of contemporary biotechnology, there is an exponential growth in the number of related information sets, necessitating cloud storage, cutting-edge management and analysis techniques, as well as adequate content protection. The worldwide, national, and local collaboration among transdisciplinary sectors and various public-private system players are only a few examples of the common, many, and diversified acts that make up the bioeconomy landscape. In addition, cyber-biosecurity concerns bring attention to an environment that is highly vulnerable and is developing quickly. Additionally, the global spread of the new virus SARS-CoV-2 has created a pandemic context that has highlighted some issues (such as the significance of strategic autonomy in supply chains for food, medical, and pharmaceutical products, the development of critical functional infrastructures, the appropriate prevention and protection measures, including the management of rapid and effective responses to pandemics or other potential malicious actions with regard to the Vulnerabilities like data confidentiality (i.e., clinical and genetic information), cloud storage, and intellectual property may present

opportunities that could be taken advantage of as science advances, depending on the application of new technologies in fields like artificial intelligence, process automation, bioinformatics, and synthetic biology. The strongest feasible cyber defense must anticipate and include potential biological threats into its procedures. This review summarizes all the aspects of new discipline of cyber-biosecurity.

1. Introduction:

Computer systems must be protected against theft, damage to their hardware, software, or data, as well as from interruption or misdirection of the services they offer. This is what cybersecurity entails. Protecting priceless biological material from abuse or damage is known as biosecurity. Cyber-biosecurity was first described by Murch et al. as "developing understanding of the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life science, cyber, cyber-physical, supply chain, and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate, and attribute such threats as it pertains to security, competitiveness, and other important considerations." Both the definitions of biosecurity and cybersecurity make an implicit value assumption about the subject matter [1-5]. We also recommend broadening this concept of cyber-biosecurity in order to set it apart from the separate purviews of cybersecurity and biosecurity. At the intersection of the life sciences and digital worlds, cyber-biosecurity addresses the potential or actual malicious destruction, misuse, or exploitation of valuable information, processes, and materials; concept mastery necessitates an understanding of this interface in the context of the threat of malicious use of technology generally[6-9]. Cross-disciplinary, cyber-biosecurity affects everything from laboratory research to environmental health, human and animal health, agriculture, and management and remediation. Technology integration has become the new standard, allowing for quick access to outdated systems like medical records through creative technological advancements and straightforward digitalization. It is becoming increasingly obvious that the domains of cybersecurity and biosecurity must also merge in order to solve innate digital and biological problems as technology disciplines expand at an exponential rate and their convergence quickens.[10, 11].

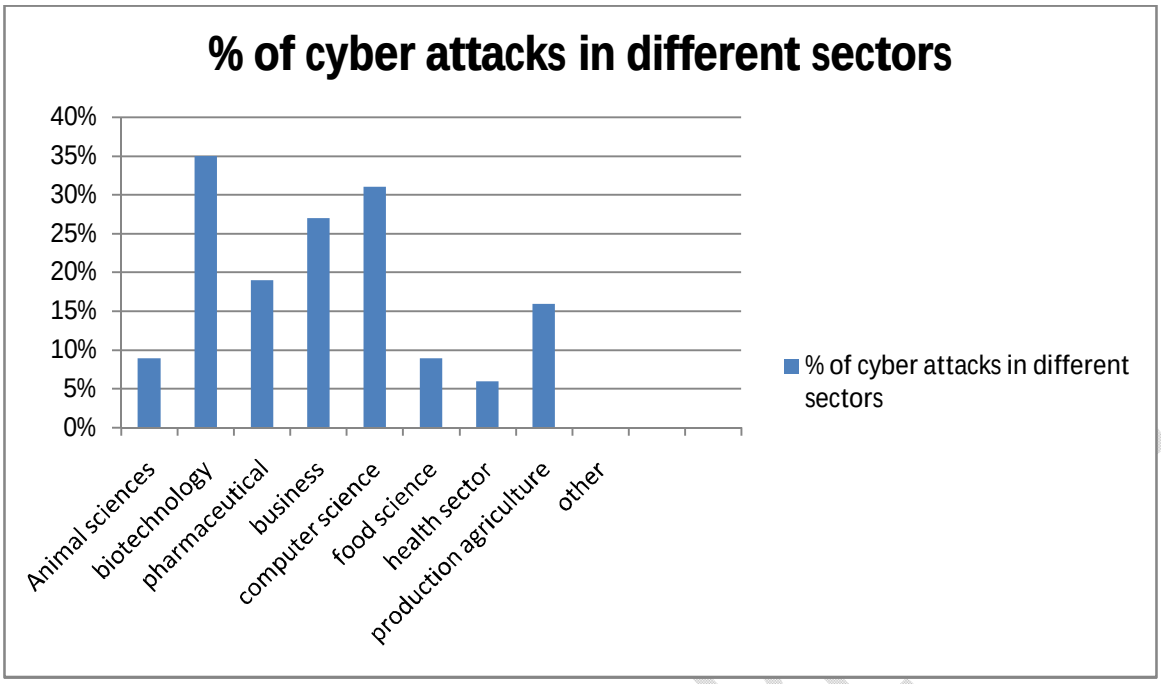


Figure 1. % of cyberattacks in different sectors

1.1.**Biosafety Vs Biosecurity**:

Biosafety and biosecurity are two distinct categories that have historically been used to classify different types of security regulations in the life sciences [12]. Policies pertaining to biosafety are developed with the purpose of preventing unintended exposure to infections as well as the inadvertent discharge of biological agents from laboratories into the surrounding environment. There are many different types of biosafety precautions, some examples of which are airlocks, sterilisation processes, and protective gear [13]. However, biosecurity rules are typically linked to topics like as international travel, supply chains, terrorist operations, and the defense sector. These regulations are intended to prevent the spread of agents that pose a risk to people's health as well as to food supply and other assets [14]. Accidental breaches of biosecurity, like a traveler bringing contaminated material back from their trip abroad, as well as purposeful breaches, like bioterrorism, are both possible [15, 16].

The regulations governing biosafety and cyber-biosecurity were developed to deal with a limited number of well-characterized biological dangers, such as controlled viruses. However, these policies do not guard against dangers that are the consequence of the deep interactions that exist between computational and experimental processes [17, 18]. It is now possible, thanks to the

development of software tools, to create DNA sequences with novel characteristics. Gene synthesis technologies have the potential to be utilised in the production of biological weapons that are generated from the genomic sequences of controlled infections. This latter discovery is what prompted the federal government to adopt screening requirements for companies that provide services related to gene synthesis . In more recent times, authorities in government agencies have voiced their worries about the potential for malicious use of genome editing technology[19, 20].

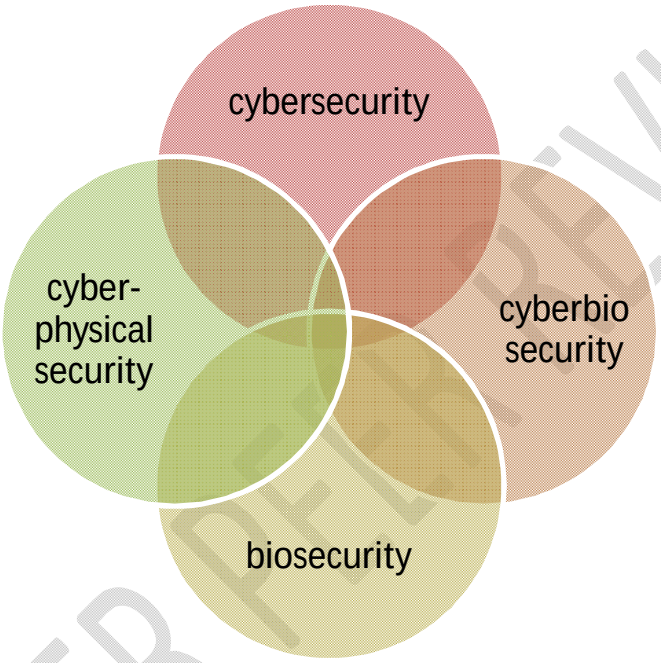


Figure 2. Cyber BioSecurity is new integrated field

1.2.Biosecurity Vs Cyber-biosecturity:

In order to secure and "prevent the loss, theft, misuse, diversion or intentional release of pathogens and toxins" [21], laboratory biosecurity is defined as the collection of practices and procedures carried out at the individual and institutional levels. Burnette's [22] definition of this term was expanded to include "products having intrinsic value, such as novel vaccines, biological therapeutics, information technology platforms, synthetic nanoparticles, or organisms, and products having high monetary value or related to biological agents" in addition to harmful biological organisms and proteins[22]. Others have provided a general definition of 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 innovation [23-25]." In this paper, we concentrate our discussion on the aspects of cyber-biosecurity that cover all types of data stored and transmitted through information technology platforms, such as data streams from networked laboratory equipment, email, electronic documents and files, databases containing sensitive business information, contracts and financial data, raw research data and its analysis, digital inventories of freezer and working stocks, digital genetic and protein data, and raw research data and its analysis.

Cyber criminals can take advantage of biosecurity flaws by stealing information from the organization's networked systems or from its contractors or employees (insiders). During the joint construction of a biosecurity program plan, IT (Information Technology) workers must take these factors into account[26, 27]. Building automation systems, facility controls, and any other networked equipment or communication systems are all at risk owing to the internet accessibility of several individual pieces of networked equipment, much as the nation's power grid and municipal utilities are [28, 29].

Access to sensitive scientific and business data as well as intellectual property of the organization is made possible by cyber infiltration of networked lab equipment and facility controls. Cyber-biosecurity invasions and data exfiltration, in addition to denial of service attacks and virus introduction, may have devastating effects on an organization's reputation and finances. These effects can put the survival of the organization in jeopardy [30, 31]. Electronic genomic and protein sequences, scientific data, intellectual property, and/or security-sensitive facility documents (such as budget documents, program plans, facility floor plans, emergency procedures, continuity of operations plans, etc.) are examples of these outcomes. They also include their destruction, theft, public disclosure, or malicious alteration [32, 33]. Access to networked laboratory tools like freezers, refrigerators, and incubators can lead to the loss of priceless chemicals and microorganisms that are in active research or experimental usage, long-term storage, or are being used as working stocks. When networked bench equipment is turned off, work time and data might be lost. Changes in the amount of light, the temperature, or the

humidity in animal rooms can stress, ill-treat, or even kill vital and pricey study animals. It is important to note that only information pertaining to the loss, theft, release, or exposure to Select Agents would be reported to the Select Agent Program—not the destruction of organisms as a result of a cyber-intrusion. This is true even if we are not aware of any particular instances like these impacting BSAT facilities [34].

The reputation of a single researcher, a primary investigator, a particular laboratory, the senior leadership of the organization, as well as the reputation of the whole company, institution, or government agency, may suffer irreversible harm as a result of these occurrences. As a result, the public, as well as present or potential students, workers, collaborators, sponsors, investors, shareholders, and funding agencies, may lose faith in the organization. Exploiting cyber-biosecurity flaws might directly endanger the existence of the life science industry [35, 36].

1.3. **What Makes Cyber-biosecurity Important**?

The integrity of developing cyber-biophysical systems and devices, such as neuromorphic computing and 3-D bio-printing, the possibility of malicious activity, such as the encoding of digitized DNA with malware, and growing security risks to cyber-biophysics are the main issues driving the call for cyber-biosecurity as a new trans-discipline. Biomechatronics, which is a branch of study that tries to combine biology, mechanics, electronics, robotics, and neurology, is another example of a cyber-biophysical invention. Turner 209 assistive, therapeutic, and diagnostic gadgets that can partially or fully replace lost human physiological processes are the subject of the field of biomegatronics. Artificial organs and tissues, prosthetic limbs, orthotics, wearable devices for physical augmentation, physical therapy and rehabilitation, robotic surgery, and natural and synthetic sensors are just a few examples of recent advancements [37-40].

2. The Digitization of Traditional Technology and Its Impact on Cyber0-biosecurity

2.1. Manufacturing

Organizations that rely heavily on science and technology are becoming increasingly complicated and networked throughout their buildings, supply chains, logistics, and transportation methods. Distributed manufacturing makes use of decentralized production

networks that are connected by information technology [41, 42]. As more links are formed between historically isolated systems, more security measures need to be addressed in order to decrease vulnerabilities and mitigate risks. The production procedures and assembly of biologics and other materials may also be dispersed and carried out asynchronously at geographically distinct places, making it possible for a response to prospective threats to be prepared in situ [43-45].

Recent advancements in cell-free metabolic engineering technology have made it possible to increase production throughput in production environments. This is in addition to easing the process of using dispersed manufacturing techniques for more traditional life science operations. As a consequence of this, biological procedures have been refined, resulting in faster prototyping and increased yields. According to Rollin et al. [46], the use of cell-free biological systems in the production of goods such as fuels, power, feed, and renewable materials is becoming increasingly common. It is becoming increasingly vital that the areas of cybersecurity and biosecurity converge in order to solve the inherent challenges that are present in both the digital and biological realms. This is due to the fast expansion of the confluence of dichotomous technology disciplines (such as automation and cellular biology), which is continuing [47, 48].

2.2.Biomedical Sciences;

As more and more health records are digitized, there is a convergence between cyber security and health security. However, this extends beyond the cyber-patient interface when it comes to electronic medical records, thus regulatory measures have been put in place to address concerns about the privacy and confidentiality of medical and billing information. A growing number of patients are having their treatment management, which may include possible medication interactions, procedures, and sensitivities that are unique to the patient, digitized [49-51]. Diagnostics and treatments that are part of personalized medicine are seeing tremendous growth, and a significant portion of the information that is linked with these interventions is stored digitally. In 2014, data breaches at three major health systems resulted in unauthorized access to millions of patient records, including clinical data[52]. This is only one example of a historical precedent for data breaches including biomedical information. Because of these breaches, the culprits had access to important clinical data, which they could either use for their own purposes or sell to make a profit. The interruption of digitally programmed diagnostic testing systems or

therapeutic targeting fields may result in unsuccessful treatment in addition to making illegal data collecting easier. Because of the various possible vulnerabilities that may be leveraged through both direct and indirect contacts with the patient and the manufacturer, medical devices are also an area of study in the field of cyber-biosecurity [53, 54].

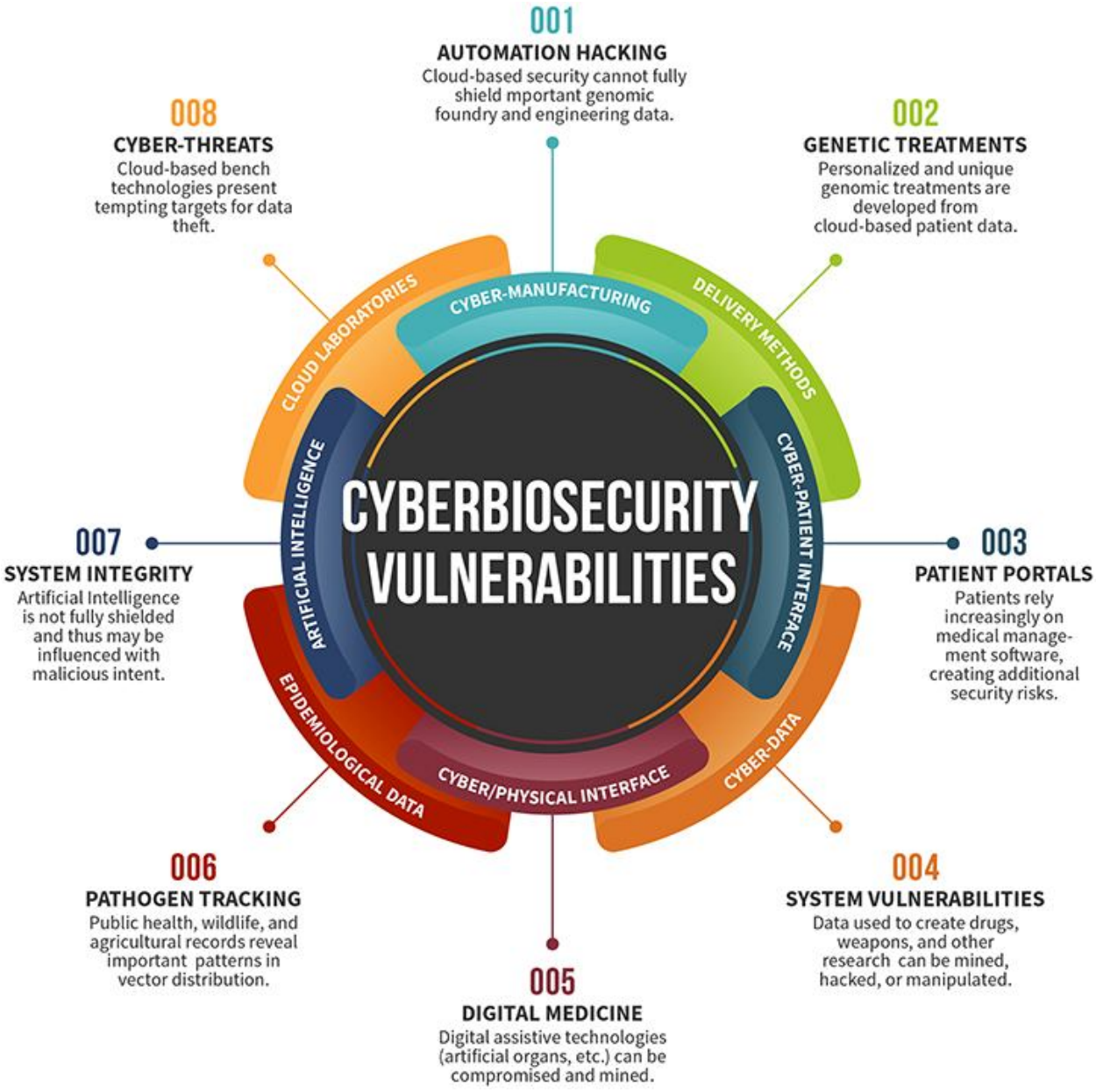
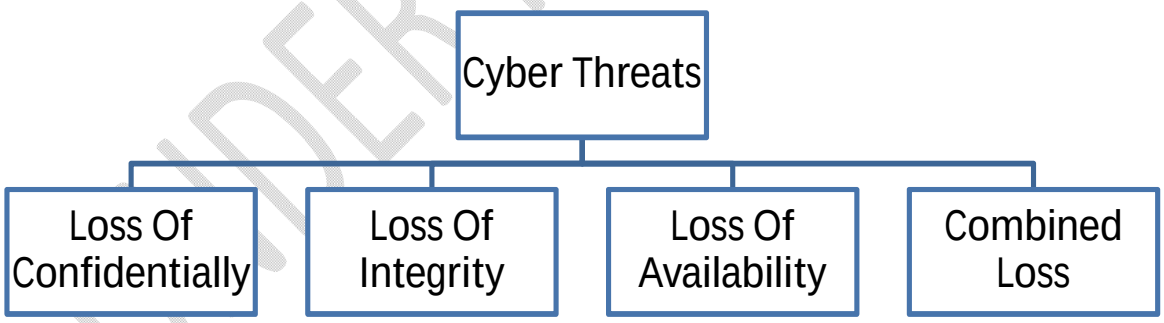


Figure 3. Cyber-Biosecurity in biomedical sector [55]

2.3.Agriculture:

In a significant portion of the world, ensuring the safety and security of food and beverages is a top responsibility. Agriculture, foodstuffs, and drinks have enormous ramifications, not only for the economy but also for the strength of society and the safety of the nation as a whole. Extensive quality control procedures have been put into place to avoid and reduce the effects of any potential hazards that may materialize [56, 57]. Outbreak and contamination detection and response systems are activated once issues are spotted. The process of labelling and packaging have also been refined and enhanced. On the other hand, many areas of farm management, production-to-consumption, raw materials-to-finished product, and logistics are dependent on cyber-enabled systems in many nations' agriculture and consumer goods industries[58, 59]. This is true for many countries. From the point of view of cyber-biosecurity, it is not obvious how this aspect of agricultural and food systems affects the health and security of those systems. In this very complex global and national environment, we reason that there must be crucial linkages and nodes that are susceptible to damage; attention must be paid to cyberbiosecurity measures is warranted and would be considerably beneficial [60, 61].

Chart 1. Types of cyber threats



3. Cyber-biosecurity In health sector:

Of course, privacy violations existed before digital health records became commonplace. While historically paper records would have been secured within hospitals and only accessible through physical breaches, the interconnectedness of today's records offers multiple potential access points, the ability to access remotely, the ability for data theft to go undetected, and access to a more complete health record providing a more valuable resource for potential attacks (whereas previously health records may have been split between many different organizations). A privacy breach may previously have affected hundreds or thousands of patients due to lost paper records or a stolen laptop, but now that this information is digitized and accessible across various networks, it could potentially affect millions of individuals [62]. To further exemplify, celebrity health records have historically been a target for hacking. The only people who could access the physical documents prior to the development of computerized records were hospital workers. Now that celebrity health information may be viewed remotely, the risk of a leak is higher. Nevertheless, the ability to track staff access to electronic information is a significant privacy advantage over paper records (a recent analysis indicates that over half of healthcare breaches originate from within the business. It is frequently simpler to monitor who has viewed electronic information than it was in the past to figure out who took a "sneak peek" at paper medical records. Although more knowledgeable/external attackers can get past this in several ways [63-66].

3.1.Cyber-Biosecurity In Biotech/Pharma Sector:

In the past, those who entered an organization to discover secrets or outright steal knowledge, data, or intellectual property posed the greatest threat to the biotech and pharmaceutical sectors. Although businesses still produce tangible goods, a large portion of their labor now takes place online, and the intellectual property, data, and information that results is now kept online [67]. Cyber security should be a business priority because if you work hard enough to produce something, you should work just as hard to safeguard it from attacks. This is especially true in an industry where the risks are high, the competition is fierce, and the rewards are frequently greater as well. According to Computer Weekly, a UK-based medical research organization was about to start working on Covid-19 vaccination trials when it was attacked by the Maze ransom ware gang. Being ready to defend oneself is a crucial consideration to take into account before

making any announcements or communicating any advances in this industry since media coverage or past triumphs might make a target where none previously existed [68].

For businesses in these rapidly evolving, high-growth industries, the rise of big data has made it feasible to collect and store enormous volumes of medical, trial, and genetic information. It should come as no surprise that the most well-known dangers are those that target data, intellectual property, or test and trial findings. Since technology both retains this information and aids much of the work being done, biotech and pharmaceutical businesses have a tendency to favor its protection, but the truth is that their security threats transcend beyond this. As an illustration, after medications are produced, there are additional dangers since raw components are sent and can be recognized, thereby releasing some of the hard-earned intellectual property. Cybercriminals that attack specific supply chain nodes in an effort to bring down the company through its suppliers can potentially interrupt production [69-72]. Given the complexity and importance of the supply chain to firms in the biotech and pharmaceutical industries, it is important to do thorough supplier due diligence in order to increase corporate security. Anything outside of your direct control should be seen as a third party risk. The boundaries of your company's cyber security don't end there, and cybercriminals are drawn to any possible weak spots in a supplier company since they might potentially impact several firms with a single assault. In a number of posts on our site, we have further information regarding protecting your supply chain [73].

Table 1. Due to such large % cyber-biosecurity is much needed

Sector	2 Breaches	3-4 Breaches
Healthcare	75%	25%
IT and telecoms	75%	24%
legal	66%	33%
HR	62%	37%
Food and agriculture	50%	50%

Another significant area of risk for companies in the biotech and pharmaceutical industries is physical security. The risk of being infiltrated by someone out to harm the business or from one

of their own employees posing an insider threat puts these businesses under even more pressure to invest in physical security measures, much like how cybercriminals can access valuable information. By doing this, an additional layer of defense will be offered that may not be necessary in other sectors of the economy. Regarding building access, degrees of data or system access, and the screening of new hires and departing employees, further layers of security could be necessary [74]. It's critical to emphasize that these risks affect all businesses, not just the bigger ones. As there appears to be no legal requirements for them to declare if they have been the subject of cyber-attacks, there is no easy way to tell how frequently these companies are being targeted. This industry has a vast worldwide network of start-up and scaleup enterprises. Being quick in this field is advantageous, but it also frequently leads to security concerns being disregarded or breached as there is frequently no dedicated resource monitoring this area. It's also likely that employees are being brought on rapidly as the company grows and that fundamental security hygiene wasn't covered during on boarding. This might pose concerns, particularly when it comes to phishing and ransom ware assaults that result in data breaches [75]. To secure data, intellectual property, and systems, it is important to use the same adaptability and flexibility as in the core business [76].

Everyone should be responsible for cyber security, and in many ways they are. However, it is impractical to expect the rest of the organization to contribute to safeguarding the business without a strong level of ownership and participation within the leadership team. This is where investing in increasing levels of awareness and expertise throughout the workforce will deliver enormous advantages because many leaders in this business may originate from the academic or scientific community and may not have a working understanding of cyber and information security [77].

There are two main ways to do this: either by hiring a Chief Information Security Officer (CISO), or, in cases where a full-time position is not required or justified, by using a virtual Chief Information Security Officer (vCISO). A virtual CISO will provide your company the expertise and experience it needs to analyze its present security posture and begin defining the steps that need to be taken to develop a cyber security plan and implement it. Along with this, training all employees should be considered a crucial component of the cyber security strategy, whether it be for the leadership team, which needs support in managing security across the entire

organization, or for the larger staff team, which has a low awareness of everyday risks and needs this to become ingrained in their roles [78-80].

3.2. **IoT Devices And Cyber-Biosecurity**:

Internet and IoT enabled knowledge sharing, networking, and global communication. "Crime harvests" [81] resulted from neglecting security. Smart meters and locks allowed burglary, stalking, and other crimes, according to 114 synthesized studies[82]. Connected health devices may represent bigger security threats than TV or fridge devices. Medical gadgets can diagnose, prevent, monitor, treat, or mitigate disease [83]. The Internet-of-Medical-Things (IoMT)—internet-connected medical-grade devices that are integrated into larger health networks to improve patient health (e.g., remote patient monitoring)—generates biological information and is transforming healthcare [84, 85]. Healthcare evolves. The UK National Health Service (NHS) published its national NHS App Library and established WiFi across its estate, allowing residents to engage with the NHS from their computer or smart phone. IoMT devices are pushed to market to satisfy the unmet need for remote patient monitoring to improve health care during the COVID19 pandemic. Security risks unintended consequences.

Figure 4. Generalized scheme of IoT and cyber-biosecurity

Insecure IoMT devices can damage patients. The NHS WannaCry ransom ware attack highlighted that security flaws may lead to data theft. The ransom ware attack in England prevented NHS personnel from accessing patient data and vital services. Applegate found a pacemaker vulnerability that permitted remote shocks. Li et al. (2011) found vulnerabilities in insulin pumps that provide daily insulin that might be used to remotely overdose patients. Two lab-demonstrated security weaknesses may constitute criminal negligence. New products can create "crime harvests". Criminals exploit vulnerabilities before they are patched. Consumer IoT device producers were urged to improve security by the UK Department for Digital, Culture, Media, and Sport (DCMS) (IoT Code of Practise & DCMS, 2018). Trustworthy manufacturers must adopt it. IoMT devices are trusted because premarket risk-management standards do not address criminal issues [86-88].

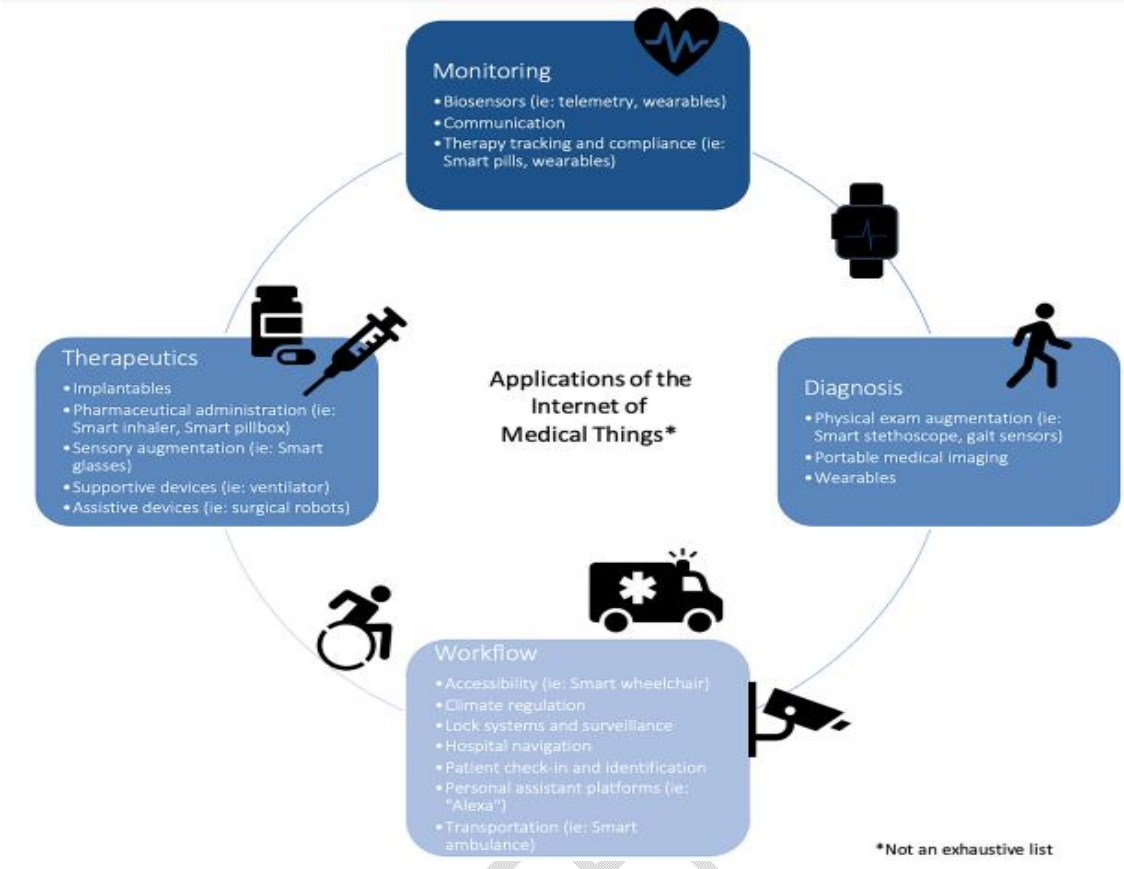


Figure 5. Applications of IoT[89]

4. Cyber-biosecurity In Agriculture:

Agriculture keeps using cutting-edge smart technologies that enable expanded remote monitoring of animals and crops. Unsupervised networks of information are produced by the connection of various technologies inside a single farm or manufacturing facility and in the data exchange between suppliers and vendors. Increased risks for cyber-security assaults on farms and agribusinesses accompany the deployment of these technologies [90]. The bioeconomy and local populations might be harmed by these attacks, which have the ability to disrupt food supply networks. The best biosecurity and cyber security policies, crucial control points, and human habits and behavior that affect overall security are all part of protecting agriculture [91]. Cyber-biosecurity is the term used to describe the intersection of these fields. Cyber-biosecurity is one of its most crucial applications, with a particular focus on the prevention of unauthorized intrusions and other activities and the protection of data, information, and other online resources pertaining to life, medical, health, agricultural, and food sciences [92, 93]. Cybersecurity

encompasses the protection of any electronic data, systems, networks, etc. It is challenging to develop policies that incorporate both information technology and life sciences since experts in one discipline sometimes lack experience in the other [94, 95]. It is challenging to educate people from secondary and post-secondary school to continuing professional development for workers of organizations since continuing professional development for employees of organizations is so new, and there are no standard training and certification courses accessible[96].

Protecting agriculture and the food supply chain is of utmost importance, particularly in light of the rising danger of food instability brought on by the Covid-19 pandemic and the quickening growth of the world's population. Sadly, it is rare for farms to have cyberattack response strategies or to understand the dangers of damaged data on decision-making. Two important elements that influence the adoption of enhanced security practices are perceived penetration risk and advantages. Agricultural workers are comparatively under-trained in biosecurity and cybersecurity, which might result in lax security procedures anywhere throughout the supply chain. Every partner in a supply chain is important because security in a chain is only as strong as its weakest link. For present and future employees, training and certifications must be developed in order to strengthen cyber-biosecurity practices generally [97, 98].

4.1.Agricultural and Food Sector Cybersecurity

Agriculture and food production and processing have been integrated among the cyber-enabled life sciences technologies with the emergence of technologies like the worldwide web. Government organizations, producers, and security specialists have therefore recognized cyber-biosecurity, particularly in the food and agricultural sector, as the answer to cyber-based threats that might possibly have catastrophic repercussions on the country's food supply chain [99]. The global market for smart farming is predicted to expand to around 26 billion dollars (USD) by 2028, with the majority of the market concentrated in North America [100]. Although advantageous, smart technology might be used by hackers to disrupt the farms that utilize them and the downstream users who depend on the supply chain. False sensor data, restricted access to data and equipment, and data encryption (i.e., ransom ware attacks) are some of the potential

dangers associated with precision agriculture and smart technology. Any of these locations may be exploited, which would jeopardize a farm's whole output. In order to start doing cyber-biosecurity research in biomanufacturing, the Department of Defense provided funding to the National Strategic Research Institute at the University of Nebraska, Colorado State University, and Virginia Tech in 2017. Their objective was to compile a list of preventative steps the sector should take to lessen its exposure to cyberattacks. Due to certain manufacturers' inability to allocate the funds required to enhancing their security, some solutions and preventative measures are unfortunately not 'one size fits all' solutions. Agriculture and security experts and professionals have turned to other cybersecurity industries to adopt and modify their practices to better match agriculture in order to build better practices [101-107].

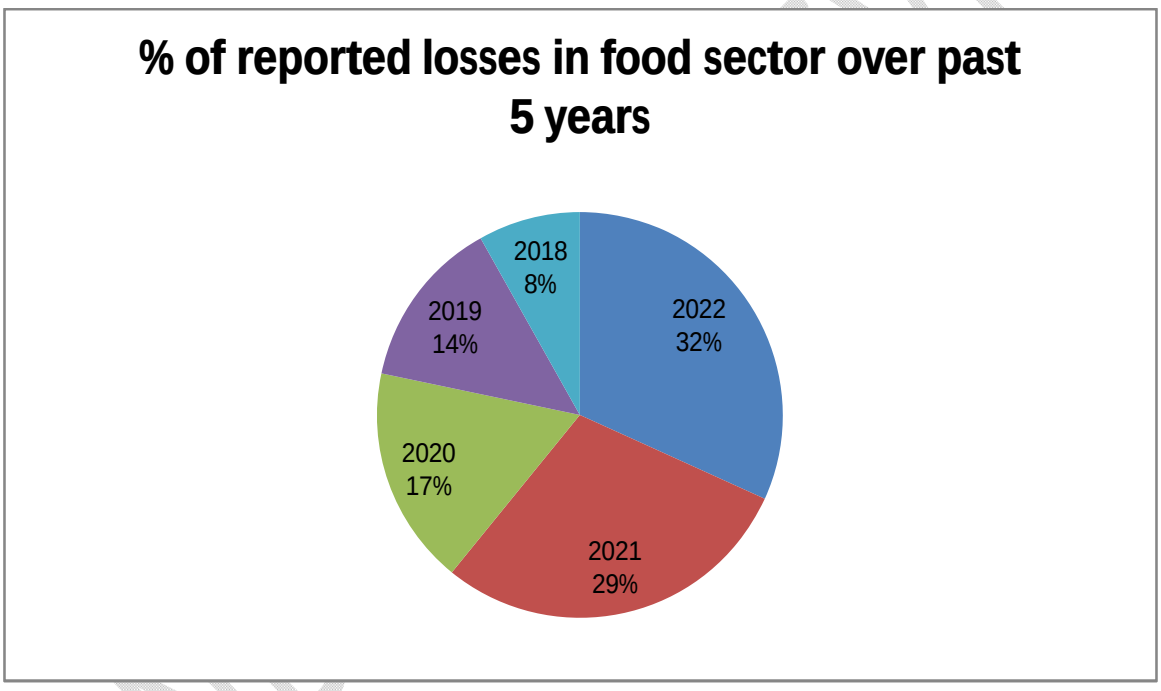


Figure 6. Losses by year in food sector due to cyber attacks

4.2.Why is there a need to worry?

Cyberattacks on the food and agriculture industries can have a detrimental impact on the supply chain as a whole, production capabilities, transportation, and product availability. A safer, more dependable supply chain will be created by comprehending the threats posed by cyber-

biosecurity and increasing awareness of vulnerabilities and mitigation techniques through the food and agriculture sector [108-110].

In the autumn of 2022, a cyberattack targeted Schreiber Foods, a Wisconsin-based producer of a range of dairy products[111, 112]. The attack disrupted the milk supply chain since all facilities had to halt operating and it took five days to recover because production plans had to be changed and supplies in transit redirected[112]. Although the facilities were back in full operation a week later, this cyber-attack was eventually to responsible for a countrywide scarcity of cream cheese that affected customers for weeks after business had resumed. Customers who wanted to prepare meals and sweets needing cream cheese were frustrated by the timing of the scarcity, which occurred around the winter holidays[112].

4.3. **What It Might Mean For Advanced Agriculture's Development/Security**:

The agriculture sector is likely to suffer harsh repercussions from competitors who have prepared for possible dangers if it does not handle existing and future concerns. Automation and remote control of agricultural machinery that may be utilized to maintain and oversee farms may one day be exploited to sabotage production and destroy a potential supply of energy. The agriculture sector may have a significant role in the energy sector. In agriculture, photosynthesis is crucial for the production of foods that are high in energy as well as for potential strategies to mitigate climate change. Synthetic and genetically modified photosynthesis may serve as a significant supply of CO2 and oxygen. New plant engineering methods are being studied because they may increase agricultural yields and increase food security. 2020 [113]. However, with increased worries about the environment and renewable energy, it is possible to hack the energy and development resources used by smart farms. Genetically modified plants and other technologies might be threatened by those who want to steal and disrupt production through hardware or software assaults. Genetically modified plants and synthetic photosynthesis could be the future of agriculture, however deployment of new technologies in agriculture would need research and budget allocation. In the midst of macro-level-induced problems that put agricultural resources in jeopardy, this risk must also be balanced. For instance, it was challenging to find basic plant seeds during the COVID-19 epidemic. This has led to a shortage of seeds, which is anticipated to have an impact on the value chain as well[114]. Similar climatic circumstances could exist in a future where climate change's severe effects are felt. Cyberattacks during these occurrences can

take advantage of technology flaws to access and take control of resources, including the genetically modified seeds. The employment of sophisticated genetic engineering technology as a weapon to take resources from farmers is possible. One speculative future scenario may take the shape of a parasite that steals DNA and threatens the privacy of targeted farms. Professor of biology Claude dePamphilis was the victim of parasitic plants that stole and used host plant genetic information as a weapon. The capacity of malevolent actors to one day use biological organisms to steal or compromise distinctive GMO intellectual property may result from this prospect. By using conventional visual methods like cameras or satellites, this hypothetical form of attack would be difficult to see. Passive monitoring devices distributed throughout farms could offer a solution to this. Active monitoring techniques that track changes in genetic material within these agricultural contexts, such as swabbing, plant cuttings, bug collecting, and frequent soil exams, might further help this [115, 116]. In the future, we could look to advancements demonstrated in dynamic, quick integrated monitoring systems.

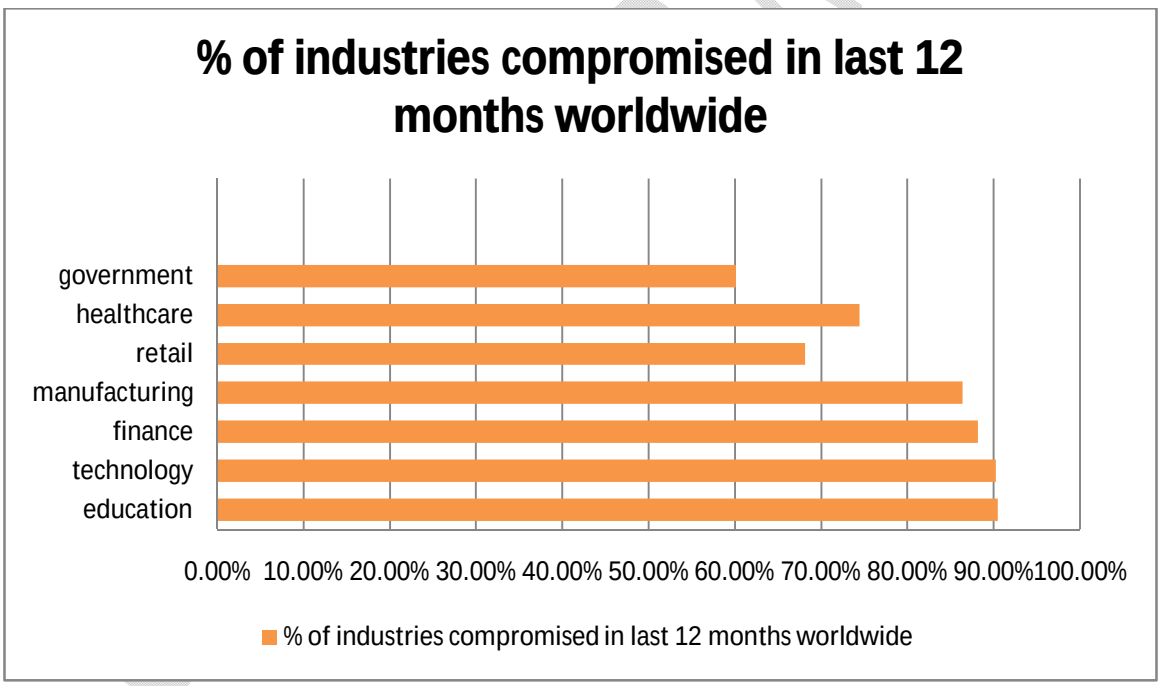


Figure 7. % of industries compromised in last 12 months worldwide

Conclusions:

It has been suggested that the fields of cyber-Biosecurity, cyber-physical security, and biosecurity, in their respective applications to biological and biomedical-based systems, should be combined under the umbrella term of cyber-biosecurity. In recent years, a variety of significant gatherings and public conversations, as well as commentary and publications, have taken place, all of which bring to light a number of different vulnerabilities? Although these are necessary first steps, they do not provide a systematized structure for effectively promoting communication, education and training, elucidation and prioritization for analysis, research, development, test and evaluation, and implementation of scientific, technological, standards of practice, policy, or even regulatory or legal considerations for the purpose of protecting the bioeconomy. In addition, professionals in the fields of biosecurity and cybersecurity are typically unaware of one other's respective domains, areas of competence, points of view, and goals, as well as the chances for mutual assistance that exist and have the potential to produce beneficial results. Developing, developing, and promoting a new field of study can help facilitate formal collaborations that are mutually beneficial and go on indefinitely. Recent important actions and publications that informed the formation of Cyber-biosecurity are briefly covered in this article. Also discussed is the extension of Cyber-biosecurity to encompass biomanufacturing, which is backed by an in-depth investigation of a biomanufacturing facility. We provide some suggestions for getting started with cyber-biosecurity and putting it on the path to become a discipline that is both well-organized and self-supporting, as well as a forum and an organization. The author's goal in writing this article was to draw attention to the emerging idea of cyber-biosecurity and to synthesise some of the key features of the confluence of the life sciences and the cyber world, which has given rise to a new, interdisciplinary area. The bioeconomy, health, and environment's contributions from biology and cyberspace are changing the security environment. Due to the current biorevolution, which is based not only on advancements in biotechnological science but also on network connections, digital DNA, and increased competitiveness, we are living in a period of new industrial trends. Business interest has advanced in the sphere of contemporary biotechnology. Artificial intelligence, global linkages, and networked systems and gadgets are all features of smart laboratories. All of the aforementioned factors create possibilities as well as dangers and weaknesses. A common language, definitions, and knowledge will help experts in

cybersecurity issues better understand the emerging field, identify security flaws, raise awareness of cyberbiological threats, and develop strategies and countermeasures. These experts are beginning to collaborate with biotechnologists or other scientific experts. The development of principles, standards, and policies to mitigate cyberattacks and other related biosecurity issues (such as dual use research, combinational weapons), with a focus on strengthening safeguarding capacities to protect human, animal, and plant health, as well as business interests, has also been called for.

References:

1. Kruse, C.S., et al., *Cybersecurity in healthcare: A systematic review of modern threats and trends.* Technology and Health Care, 2017. **25**(1): p. 1-10.
2. Ross, R.S., L. Feldman, and G.A. Witte, *Rethinking Security through Systems Security Engineering.* 2016.
3. Fernández, Ò.S., et al., *Shared Medical Record, Personal Health Folder and Health and Social Integrated Care in Catalonia: ICT Services for Integrated Care.* InNew Perspectives in Medical Records, 2017: p. 49-64.
4. Kam, R., *The human risk factor of a healthcare data breach-Community Blog.* Heal. IT Exch, 2015.
5. Arndt, R., *In healthcare, breach dangers come from inside the house.* Mod. Healthc, 2018.
6. Dimitrov, D.V., *Medical internet of things and big data in healthcare.* Healthcare informatics research, 2016. **22**(3): p. 156-163.
7. Filkins, B.L., et al., *Privacy and security in the era of digital health: what should translational researchers know and do about it?* American journal of translational research, 2016. **8**(3): p. 1560.
8. Abelson, R. and M. Goldstein, *Anthem hacking points to security vulnerability of health care industry.* The New York Times, February, 2015.
9. Kangas, E., *Why Are Hackers Targeting Your Medical Records?, 2017*.
10. Walker, T., *Interoperability a must for hospitals, but it comes with risks, Manag.* Healthc. Exec, 2017.
11. Shenoy, A. and J.M. Appel, *Safeguarding confidentiality in electronic health records.* Cambridge Quarterly of Healthcare Ethics, 2017. **26**(2): p. 337-341.
12. *C. Szegedy et al., Intriguing properties of neural networks. arXiv [cs.CV] (2013).*
13. *A. Nguyen, J. Yosinski, J. Clune, Deep neural networks are easily fooled: High confidence predictions for unrecognizable images, in Proceedings of the IEEE conference on computer vision and pattern recognition (2015), pp. 427–436.*
14. *P. Jurcys, C. Donewald, M. Fenwick, M. Lampinen, A. Smaliukas, Ownership of user-held data: Why property law is the right approach. Harv. J. Law Technol. Digest (2020). https://doi.org/10.2139/ssrn.3711017.*
15. *L. Sweeney, A. Abu, J. Winn, Identifying participants in the personal genome project by name. 2013. Available at SSRN (2013).*
16. *Y. Nakamura et al., KART: Parameterization of privacy leakage scenarios from pre-trained language models. arXiv [cs.CL] (2020).*

17. *D.C. Barth-Jones, The 're-identification' of Governor William Weld's medical information: A critical re-examination of health data identification risks and privacy protections, then and now. SSRN Electron. J.* https://doi.org/10.2139/ssrn.2076397.
18. *A. Narayanan, V. Shmatikov, Robust de-anonymization of large sparse datasets, in 2008 IEEE Symposium on Security and Privacy (sp 2008) (2008), pp. 111–125.*
19. *Robert Philipp Economics and Statistics, University of Vienna, Austria, Andreas Mladenow Economics and Statistics, University of Vienna, Austria, Christine Strauss Economics and Statistics, University of Vienna, Austria & Alexander Völz Economics and Statistics, University of Vienna, Austria. Machine Learning as a Service. ACM Other conferences* https://dl.acm.org/doi/abs/10.1145/3428757.3429152.
20. *Manish Kesarwani IBM Research, India, Bhaskar Mukhoty Indian Institute of Technology, Kanpur, Vijay Arya IBM Research, India & Sameep Mehta IBM Research, India. Model Extraction Warning in MLaaS Paradigm. ACM Other conferences* https://dl.acm.org/doi/abs/10.1145/3274694.3274740.
21. *A. Meiseles, I. Rosenberg, Y. Motro, L. Rokach & J. Moran-Gilad, Adversarial vulnerability of deep learning models in analyzing next generation sequencing data, in 2020 IEEE International Conference on Bioinformatics and Biomedicine (BIBM) (IEEE, 2021).* https://doi.org/10.1109/BIBM49941.2020.9313421.
22. *A. Aminifar, Minimal adversarial perturbations in mobile health applications: The epileptic brain activity case study, in ICASSP 2020–2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (2020), pp. 1205–1209.*
23. *S. Bhambri, S. Muku, A. Tulasi, A.B. Buduru, A survey of black-box adversarial attacks on computer vision models. arXiv [cs.LG] (2019).*
24. *R. Shokri, M. Stronati, C. Song, V. Shmatikov, Membership inference attacks against machine learning models, in 2017 IEEE Symposium on Security and Privacy (SP) (2017), pp. 3–18.*
25. *Y. Long et al., Understanding membership inferences on well-generalized learning models. arXiv [cs.CR] (2018).*
26. *M. Nasr, R. Shokri, A. Houmansadr, Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning, in 2019 IEEE Symposium on Security and Privacy (SP) (2019).* https://doi.org/10.1109/sp.2019.00065.
27. *M. Fredrikson, S. Jha, T. Ristenpart, Model inversion attacks that exploit confidence information and basic countermeasures, in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1322–1333 (Association for Computing Machinery, 2015).*
28. *A. Salem, A. Bhattacharya, M. Backes, M. Fritz, Y. Zhang, ${Updates-Leak}$: Data set inference and reconstruction attacks in online learning, in 29th USENIX Security Symposium (USENIX Security 20) (2020), pp. 1291–1308.*
29. *F. Tramèr, F. Zhang, A. Juels, M.K. Reiter, T. Ristenpart, Stealing machine learning models via prediction ${APIs}$, in 25th USENIX security symposium (USENIX Security 16) (2016), pp. 601–618.*
30. *B. Wang, N.Z. Gong, Stealing hyperparameters in machine learning, in 2018 IEEE Symposium on Security and Privacy (SP) (2018), pp. 36–52.*
31. *G. Sivathanu, C.P. Wright, E. Zadok, Ensuring data integrity in storage: Techniques and applications. in Proceedings of the 2005 ACM workshop on Storage security and survivability (Association for Computing Machinery, 2005), pp. 26–36.*
32. *M. Jegorova et al., Survey: Leakage and privacy at inference time. arXiv [cs.LG] (2021).*
33. *Nakamoto, Bitcoin: A peer-to-peer electronic cash system. Decentralized Bus. Rev. 21260 (2008).*

34. *M. Mettler, Blockchain technology in healthcare: The revolution starts here, in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), (2016), pp. 1–3.*
35. *R. Jabbar, N. Fetais, M. Krichen, K. Barkaoui, Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity, in 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (2020), pp. 310–317.*
36. *Guardtime Health. https://m.guardtime.com/files/Guardtime_whitepaper_A4_april_web.pdf.*
37. *X. Liu et al., Privacy and security issues in deep learning: A survey. IEEE Access 9, 4566–4593. (undefined 2021).*
38. *X. Liu, M. Cheng, H. Zhang, C.-J. Hsieh, Towards robust neural networks via random self-ensemble, in Proceedings of the European Conference on Computer Vision (ECCV) (2018), pp. 369–385.*
39. *M. Lecuyer, V. Atlidakis, R. Geambasu, D. Hsu, S. Jana, Certified robustness to adversarial examples with differential privacy, in 2019 IEEE Symposium on Security and Privacy (SP) (2019), pp. 656–672.*
40. *S.R.M. Oliveira, O.R. Zaiane, Protecting sensitive knowledge by data sanitization, in Third IEEE International Conference on Data Mining (2003), pp. 613–616.*
41. *F.M. Chan et al., Genotype imputation with homomorphic encryption, in 2021 6th International Conference on Biomedical Signal and Image Processing (Association for Computing Machinery, 2021), pp. 9–13.*
42. *A.C. Yao, Protocols for secure computations, in 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982) (1982), pp. 160–164.*
43. *J.I. Choi, K.R.B. Butler, Secure multiparty computation and trusted hardware: Examining adoption challenges and opportunities. Secur. Commun. Netw. 2019 (2019).*
44. *C. Shepherd et al., Secure and trusted execution: Past, present, and future – A critical review in the context of the internet of things and cyber-physical systems, in 2016 IEEE Trustcom/BigDataSE/ISPA (2016), pp. 168–177.*
45. *I. Anati, S. Gueron, S. Johnson, V. Scarlata, Innovative technology for CPU based attestation and sealing, in Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy vol. 13 (ACM New York, 2013).*
46. *NVIDIA, NVIDIA H100 tensor core GPU architecture overview. https://resources.nvidia.com/en-us-tensor-core (2022).*
47. Acar, A., et al., *A survey on homomorphic encryption schemes: Theory and implementation.* ACM Comput. Surv., 2018. **51**.
48. Battista Biggioab, F.R., *Wild patterns: Ten years after the rise of adversarial machine learning.* Pattern Recognit., 2018. **84**.
49. Chen, F., *PRESAGE: PRivacy-preserving gEnetic testing via SoftwAre Guard Extension.* BMC Med. Genom., 2017. **10**.
50. Chen, F., *PRINCESS: Privacy-protecting rare disease international network collaboration via encryption through software guard extension S.* Bioinformatics, 2017. **33**.
51. Cramer, R., I.B. Damgard, and J.B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. 2015: Cambridge University Press.
52. Dwork, C., et al., *Calibrating noise to sensitivity in private data analysis.* J. Priv. Confid., 2017. **7**.
53. Dwork, C. and A. Roth, *The algorithmic foundations of differential privacy.* Found. Trends Theor. Comput. Sci., 2013. **9**.
54. Finlayson, S.G., *Adversarial attacks on medical machine learning.* Science, 2019. **363**.
55. Richardson, L.C., et al., *Cyberbiosecurity: A Call for Cooperation in a New Threat Landscape.* Frontiers in Bioengineering and Biotechnology, 2019. **7**.

56. Gentry, C., *A Fully Homomorphic Encryption Scheme*. 2009: Stanford University.
57. Gürsoy, G., *Data sanitization to reduce private information leakage from functional genomics.* Cell, 2020. **183**.
58. Gürsoy, G., *Functional genomics data: Privacy risk assessment and technological mitigation.* Nat. Rev. Genet., 2022. **23**.
59. Gürsoy, G., et al., *Privacy-preserving genotype imputation with fully homomorphic encryption.* Cell Syst., 2022. **13**.
60. Gymrek, M., et al., *Identifying personal genomes by surname inference.* Science, 2013. **339**.
61. Harmanci, A. and M. Gerstein, *Quantification of private information leakage from phenotype-genotype data: Linking attacks.* Nat. Methods, 2016. **13**.
62. Hummel, P., M. Braun, and P. Dabrock, *Own Data? Ethical reflections on data ownership.* Philos. Technol., 2021. **34**.
63. Iwendi, C., *N-Sanitization: A semantic privacy-preserving framework for unstructured medical datasets.* Comput. Commun., 2020. **161**.
64. Joly, Y., et al., *Are data sharing and privacy protection mutually exclusive?* Cell, 2016. **167**.
65. Khan, S.I. and A.S.M. Hoque, *Digital health data: A comprehensive review of privacy and security risks and some recommendations.* Comput. Sci. J. Moldova, 2016. **24**.
66. Kim, M., *Ultrafast homomorphic encryption models enable secure outsourcing of genotype imputation.* Cell Syst., 2021. **12**.
67. Greenbaum, D., *An analysis of federal circuit discrimination: The evolution of the written description requirement vis-a-vis DNA and biotechnological inventions concerns for synthetic biology.* Recent Patents DNA Gene Seq. (Discont.), 2011. **5**.
68. Greenbaum, D., *Avoiding overregulation in the medical internet of things*, in *Big Data, Health Law and Bioethics*. 2018, Cambridge University Press.
69. Greenbaum, D., *Biology's brave new world.* Science, 2020. **369**.
70. Harmanci, A. and M. Gerstein, *Analysis of sensitive information leakage in functional genomics signal profiles through genomic deletions.* Nat. Commun., 2018. **9**.
71. Hayden, E.C., *Privacy protections: The genome hacker.* Nature, 2013. **497**.
72. Homer, N., *Resolving individuals contributing trace amounts of DNA to highly complex mixtures using high-density SNP genotyping microarrays.* PLoS Genet., 2008. **4**.
73. Greenbaum, D., *Making compassionate use more useful: Using real-world data, real-world evidence and digital twins to supplement or supplant randomized controlled trials*, in *Biocomputing 2021: Proceedings of the Pacific Symposium*. 2020.
74. Greenbaum, D., *Cyberbiosecurity: An emerging field that has ethical implications for clinical neuroscience.* Camb. Q. Healthc. Ethics, 2021. **30**.
75. Greenbaum, D., et al., *Interrelating different types of genomic data, from proteome to secretome: 'Oming in on function'.* Genome Res., 2001. **11**.
76. Liv, N. and D. Greenbaum, *Cyberneurosecurity*, in *Policy, Identity and Neurotechnology: The Neuroethics of Brain-Computer-Interfaces*, V. Dubljevi and A. Coin, Editors. 2023.
77. Oeschger, F.M. and U. Jenal, *Addressing the misuse potential of life science research – Perspectives from a bottom-up initiative in Switzerland*, in *Gain of Function Research of Concern*, D. Greenbaum and K. Berns, Editors. 2018.
78. Puzis, R., et al., *Increased cyber-biosecurity for DNA synthesis.* Nat. Biotechnol., 2020. **38**.
79. Sherman, M., Z. Idan, and D. Greenbaum, *Who watches the step-watchers: The ups and downs of turning anecdotal citizen science into actionable clinical data.* Am. J. Bioeth., 2019. **19**.
80. Yu, H., et al., *TopNet: A tool for comparing biological sub-networks, correlating protein properties with topological statistics.* Nucleic Acids Res., 2004. **32**.

81. Almilaji, O., et al., *The development of a clinical decision-support web-based tool for predicting the risk of gastrointestinal cancer in iron deficiency anaemia—the IDIOM app.* Digital, 2022. **2**.
82. Beckers, R., Z. Kwade, and F. Zanca, *The EU medical device regulation: Implications for artificial intelligence-based medical device software in medical physics.* Physica Medica, 2021. **83**.
83. Ben-Menahem, S.M., et al., *How the new European regulation on medical devices will affect innovation.* Nature Biomedical Engineering, 2020. **4**.
84. Bhatia, R.S., K.G. Shojania, and W. Levinson, *Cost of contact: Redesigning healthcare in the age of COVID.* BMJ Quality & Safety, 2021. **30**.
85. Blythe, J.M. and S.D. Johnson, *A systematic review of crime facilitated by the consumer Internet of Things.* Security Journal, 2021. **34**.
86. Elgabry, M., D. Nesbeth, and S. Johnson, *The future of biotechnology crime: A parallel delphi study with non-traditional experts.* Futures, 2022. **141**.
87. Ghafur, S., et al., *The challenges of cybersecurity in health care: The UK National Health Service as a case study.* The Lancet Digital Health, 2019. **1**.
88. Han, J.E.D., et al., *Opportunities and risks of UK medical device reform.* Therapeutic Innovation & Regulatory Science, 2022.
89. Elgabry, M., *Towards cyber-biosecurity by design: an experimental approach to Internet-of-Medical-Things design and development.* Crime Science, 2023. **12**(1): p. 3.
90. *Australian Government, (2020). Australia's Cyber Security Strategy 2020. Canberra: Commonwealth of Australia.*
91. *Barrett, D. (2015). U.S. Plans to Use Spy Law to Battle Corporate Espionage. The Wall Street Journal, July 23rd. Available online at: https://www.wsj.com/articles/u-s-plans-to-use-spy-law-to-battle-corporate-espionage-1437688169 (accessed February 25, 2021).*
92. *Bajema, N., DiEuliis, D., Lutes, C., & Lim, Y. (2018). The Digitization of Biology: Understanding the New Risks and Implications for Governance, Technical Report, Washington, DC, National Defense University. Center for the Study of Weapons of Mass Destruction.*
93. *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). https://doi.org/10.3389/fbioe.2019.00021.*
94. *DiEuliis, D., & Giordano, J. (2017). Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. Health security, 15(3), 296–302.*
95. *Diggans, J., & Leproust, E. (2019). Next Steps for Access to Safe, Secure DNA Synthesis, Frontiers in Bioengineering and Biotechnology 7 (86). https://doi.org/10.3389/fbioe.2019.00086.*
96. *Erman, M., & Finkle, J. (2017). Merck Says Cyber Attack Halted Production, Will Hurt Profits. Reuters. Available online at: https://www.reuters.com/article/us-merck-co-results/merck-says-cyber-attack-halted-production-will-hurtprofits-idUSKBN1AD1AO.*
97. *Eshoo, A., & Schiff, A. (2019). "China's grip on pharmaceutical drugs is a national security issue," The Washington Post, September 10. https://www.washingtonpost.com/opinions/we-rely-on-china-forpharmaceutical-drugs-thats-a-security-threat/2019/09/10/5f35e1ce-d3ec-11e9-9343-40db57cf6abd_story (accessed 25th February 2021).*
98. *Fair, P., & Farrant, G. (2019). "Australian Government Announces a Foreign Interference Taskforce for Universities," Global Compliance News. Backer McKenzie, 19 September.*
99. *George, A. M. (2019). The National Security Implications of Cyberbiosecurity. Frontiers in Bioengineering and Biotechnology, 7(51). https://doi.org/10.3389/fbioe.2019.00051.*
100. *Greenwood, J. C. (2013). Biotech in China. European Biopharmaceutical Review (Winter): 62–64.*
101. *Guttieres, D., Stewart, S., Wolfrum, J., & Springs, S. (2019). Cyberbiosecurity in Advanced Manufacturing Models, Frontiers in Bioengineering and Biotechnology 7 (210). https://doi.org/10.3389/fbioe.2019.00210.*

102. *Heinemann, J. A., & Walker, S. (2019). Environmentally applied nucleic acids and proteins for purposes of engineering changes to genes and other genetic material. Biosafety and Health, 1(03), 113–123.*
103. *Kania, E., & Wilson, V. (2019).“Weaponizing Biotech: How China’s military is preparing for a ‘new domain of warfare,’” Defense One, August 14, 2019, https://www.defenseone.com/ideas/2019/08/chinasmilitary-pursuing-biotech/159167.*
104. *Knapp, B. (2018). Fifth Domain, Researchers are Sounding the Alarm on Cyberbiosecurity. https://www.fifthdomain.com/dod/2018/02/08/researchers-are-sounding-thealarm-on-cyberbiosecurity/ (accessed 20 April 2020).*
105. *Lawless, J. & Kirka, D. (2020). ‘UK, US, Canada Accuse Russia of Hacking Virus Vaccine Trials’. TechXplore (July 16). https://techxplore.com/news/2020-07-uk-canada-accuse-russia-hacking.html?utm_source=TrendMD&utm_medium=cpc&utm_campaign=TechXplore.com_TrendMD_1 (accessed 24th February 2021).*
106. *Marsh, S. (2018). US joins UK in Blaming Russia for NotPetya Cyber-attack. The Guardian, 15(02), 2018. Available online at: https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine (accessed 24th February 2021).*
107. *Millett, K., dos Santos, E., & Millett, P. D. (2019). Cyber-biosecurity Risk Perceptions in the Biotech Sector, Frontiers in Bioengineering and Biotechnology 7 (136). https://doi.org/10.3389/fbioe.2019.00136.*
108. *Moritz, R. L., Berger, K. M., Owen, B. R., & Gillum, D. R. (2020). Promoting biosecurity by professionalizing biosecurity. Science, 367(6480), 856–858. https://doi.org/10.1126/science.aba0376.*
109. *Mueller, S. (2020). Facing the 2020 Pandemic: What Does Cyberbiosecurity Want Us to Know to Safeguard the Future? Biosafety and Health. https://doi.org/10.1016/j.bsheal.2020.09.007.*
110. *Murch, R., & DiEuliis, D. (2019). Editorial: Mapping the Cyberbiosecurity Enterprise. Frontiers in Bioengineering and Biotechnology 7 (235). https://doi.org/10.3389/fbioe.2019.00235.*
111. *Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. Frontiers in Bioengineering and Biotechnology, 6(39). https://doi.org/10.3389/fbioe.2018.00039.*
112. *National Academies of Sciences, Engineering, and Medicine. (2020). Safeguarding the Bioeconomy. Washington, DC: The National Academies Press. https://doi.org/10.17226/25525.*
113. *White House. (2021a) National Strategy for COVID-19 Response and Pandemic Preparedness, (January), Washington, DC.*
114. *White House. (2021b). National Security Memorandum on U.S Global Leadership to Strengthen the International COVID-19 Response and Advance Global Security, (January), Washington, DC.*
115. *Wintle, B. C., Boehm, C. R., Rhodes, C., Molloy, J. C., Millett, P., Adam, L.,... & Sutherland, W. J. (2017). Point of View: A transatlantic perspective on 20 emerging issues in biological engineering. Elife, 6, e30247.*
116. Javorcik, B., *Global Supply Chains Will Not Be the Same in the Post-COVID-19 World*, in *COVID-19 and Trade Policy: Why Turning Inward Won’t Work*, R. Baldwin and S. Evenett, Editors. 2020, CEPR Press: London.